HACKER JOURNAL

Anno 1 - N. 9
26 settembre/10 ottobre 2002

Boss: theguilty@hackerjournal.it

Publisher: ilcoccia@hackerjournal.it

Editor: grAnd@hackerjournal.it,

Graphic designer: Michele Lovison, Karin Harrop

Contributors: Bismark.it, Tuono Blu, Onda Quadra,

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco sul Naviglio
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00187 Roma - Piazza Colonna, 361- Tel. 06.69514.1 r.a.
20134 Milano, via Cavriana, 14
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.

Direttore responsabile:
Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. Parola di hacker. SCRIVETE!!!

redazione@hackerjournal.it

hack·er (hăk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

ROCCO TAROCCO È VIVO E LOTTA INSIEME A NOI

Nei giorni scorsi ha fatto la sua comparsa in televisione e sulle radio una nuova campagna pubblicitaria di Universal Music; una di quelle che sarà costata milioni di euro e ore di riunioni tra creativi, sociologi, studiosi delle tendenze giovanili (i famigerati "cool hunter", che girano per le città spiando le abitudini dei ragazzi per scoprire che cosa fa tendenza). Tutto questo "sforzo" ha prodotto un paio di spot, nei quali il brufoloso e occhialuto adolescente Rocco Tarocco viene sbeffeggiato dagli amici e piantato dalla ragazza a causa di CD musicali copiati.

Nel primo spot, Rocco ha una bancarella di dischi pirata, che cerca di vendere strillando come al mercato del pesce; passano gli amici, e gli dicono che "gli originali sono un'altra cosa, e che ormai non costano poi tanto". Il biasimo ci può anche stare, perché Rocco sta vendendo i CD (ma tra chi vende CD per strada, quanti adolescenti ben vestiti avete visto?). Anche l'elogio dell'originale, completo di booklet e copertina, si comprende. Ma dire che i dischi non costano tanto, è una bestialità (se si escludono particolari promozioni, come quella che la stessa Universal fa di questi tempi; un CD a 5 euro). A questo punto, forse avrebbe avuto più effetto una campagna che puntasse tutto sull'abbassamento del prezzo, invece del surreale siparietto di Rocco che vende CD per strada (Hey, Universal, vi do un suggerimento: i ragazzi i CD non li vendono, se li scambiano gratuitamente).

Vuoi sapere se la tua ragazza (o il tuo ragazzo) ti ama davvero? Regalae un CD copiato!

Ma è con il secondo spot che si raggiunge veramente il livello più basso. Rocco regala alla fidanzata un CD per il suo compleanno. Lei lo prende, lo osserva ed esclama: "ma questo è un tarocco; tu non ci tieni veramente a me". Detto ciò gli ammolla uno schiaffone e lo lascia. Il messaggio è evidente: nelle relazioni tra ragazzi, non importano l'affetto, le persone, o il fatto di scambiarsi pensieri gentili. L'unica cosa che conta è potersi permettere di comprare CD originali a profusione.

Noi preferiamo trovare un'altra morale per lo spot di Rocco Tarocco: vuoi sapere se la tua ragazza ti ama davvero? Regalale un CD che hai fatto da solo, selezionando con cura i brani uno a uno, e stampando una copertina con una dedica unica. Se si comporta come la ragazza di Rocco, significa che di te non gliene fregava un gran che, e non ci hai perso molto.

grand@hackerjournal.it

NEWS

HOT!

IN GRECIA SI TORNA A GIOCARE

La tanto discussa legge che vietava di usare videogiochi in pubblico, entrata in vigore alcune settimane fa in Grecia, **è stata finalmente giudicata incostituzionale e annullata**. Rimane il divieto di utilizzare video poker e di visitare casinò online, ma gli sparatutto da sala sono finalmente tornati legali. Chi ha voglia di organizzare un Lan party alle pendici del monte Olimpo?

BRUCE PERENS LICENZIATO DA HP

Nello scorso numero parlavamo degli screzi tra HP e un suo dipendente molto particolare, il guru Open Source Bruce Perens. Sarà che qualcuno ai piani alti si è arrabbiato, sarà che Bruce mordeva il freno, ma la situazione si è risolta in modo drastico. **HP e Perens hanno annunciato il divorzio**; secondo le affermazioni dello stesso Bruce, sembrerebbe che la separazione sia avvenuta in modo tutto sommato consensuale.
Tra i progetti di cui Bruce Perens si sta occupando attualmente, segnaliamo quello per una Scelta Sincera del software (**http://sincerechoice.com**), che punta a stabilire criteri per **limitare i monopoli industriali e favorire l'utilizzo di standard e formati di file aperti**.

PIG IN JAPAN

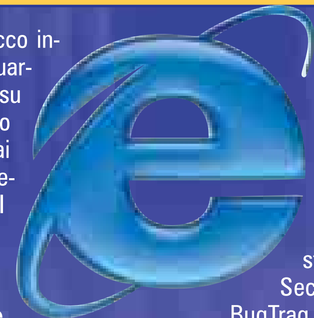
Per arrivare alla fine del mese, due studentesse giapponesi non hanno esitato a rivolgersi a un sito di incontri. Vivevano di pubblicità? No, affatto, **si sono consegnate alla prostituzione e al racket**. Secondo un'inchiesta condotta dalla polizia su più di 2.000 studenti, sembra che circa uno su dieci prenda appuntamenti attraverso siti di incontri. Per le dodici ragazze arrestate quella sarebbe la prima esperienza di questo tipo, secondo quanto hanno dichiarato. Altre ragazze avrebbero fatto ricorso a Internet per vendere i propri corpi. Il pretesto sarebbe la vendita di biancheria intima, ma le transazioni possono andare ben più lontano e per soli 5.000 yen. **Il numero di arresti per prostituzione di bambini o di adolescenti in Giappone è passato da 5 nel 2000 a 117 nel 2001.**

XBOX LINUX, UN PROGETTO PROMETTENTE



Voi l'avete sognato, loro l'hanno fatto. Foraggiati da un finanziamento di $ 200.000, decine di sviluppatori indipendenti hanno accettato **la sfida della trasformazione di un Xbox in un calcolatore GNU/Linux**.
Dall'immaginazione degli sviluppatori è già uscito un bios e il progetto prosegue. L'interesse della prodezza? Una volta modificata, questa Xbox varrà molto più del suo prezzo attuale, grazie ai programmi liberi. E poi volete mettere la soddisfazione di vedere la reazione di Zio Bill quando questi ragazzi riusciranno a installare **un Linux funzionante proprio sul primo giocattolino hardware prodotto da Microsoft?**
Per saperne di più:
http://xbox-linux.sourceforge.net/

FINIRANNO MAI I BACHI DI EXPLORER?



Non è facile trovare un attacco intrigante per una notizia riguardante la scoperta di un baco su Internet Explorer, soprattutto quando di notizie simili ne hai scritte una trentina nel corso degli anni, ma così è la vita. Il punto è questo: il gruppo Grey Magic Software ha scoperto che **sfruttando i tag <frame> e <iframe> è possibile far eseguire codice a piacere sul computer di chiunque acceda a una pagina Web** appositamente confezionata a questo scopo.
Il bello è che Gray Magic Software aveva avvisato Microsoft del problema molto prima del rilascio del Service Pack 1 per IE 6 ma, indovinate, **il "pacco" non risolve assolutamente questo problema**. Trascorso un mese, come di consuetudine in questi casi, Gray Magic Software ha reso pubblica la falla.
Ma Explorer non è il solo software Microsoft a essere sotto la lente in questi giorni; un importante falla che minaccia la privacy degli utenti è stata scoperta anche in Word. Secondo quanto affermato da BugTraq, è possibile confezionare un documento di Word in modo che, spedito a un'altra persona, **prelevi un file qualsiasi dall'hard disk di un utente e lo ingolobi al suo interno**, in modo completamente invisibile. Se un attaccante quindi inviasse un documento succhia dati a un'altra persona, e la convincesse a fare qualche modifica al file e poi rispedirlo al mittente, potrebbe entrare in possesso di file riservati presenti sul computer della vittima.

PROPOSTA INDECENTE PER NAPSTER

**Il porno editore Private Media Group (www.prvt.com) ha offerto un milione delle sue azioni, corrispondenti a un valore di 2,4 milioni di dollari, per acquistare il marchio e il dominio Internet di Napster, allo scopo di realizzare un sistema di file sharing tutto dedicato a immagini e filmati erotici.
In questo modo, Private spera di aumentare il numero di utenti che si abbonano ai propri servizi online o comprano riviste e video. Chissà se Private ricorda che Bertlesmann aveva comprato Napster, pagandolo 15 milioni di dollari e investendone altri 85, proprio con lo scopo di aumentare le vendite dei suoi dischi, per finire poi col mettere il sistemone in naftalina?**

STUDENTE DEBIAN... PRESENTE!

Ricominciano le scuole, e quest'anno all'appello si è presentato un nuovo studente: DebianEdu, un progetto che si pone di **adattare il più possibile la distribuzione GNU/Linux Debian al mondo della scuola**. Il tutto dovrebbe avvenire attraverso la realizzazione di pacchetti appositamente studiati per la scuola; si stanno sviluppando moduli software su **astronomia, elettronica, grafica, linguaggio, matematica, musica, fisica, chimica e altre materie**. Linux è già abbondantemente diffuso nelle facoltà tecniche delle università, ma stenta un po' a decollare nelle materie umanistiche e nelle scuole elementari, medie e superiori. La speranza è quindi che questo progetto possa dare una spinta al sistema del pinguino in quegli ambienti tradizionalmente dominati da Microsoft e da Apple (soprattutto negli Stati Uniti, dove Apple ha una posizione di tutto rispetto nel mercato educational.

Per saperne di più, schizzate su

http://wiki.debian.net/DebianEdu

TISCALI PASSA A V.92

A grande distanza di tempo dall'introduzione di V.92, sembrava che questo protocollo per i modem analogici dovesse morire senza essere mai implementato, per lo meno in Italia. **Tiscali invece ha aggiornato i propri punti di accesso per supportare questo protocollo**. Tra i principali miglioramenti offerti da V.92 ricordiamo **l'aumento della velocità in upload** fino a 48.000 bps (contro gli attuali 33.600 bps), **tempi di collegamento più veloci** e la possibilità di **mettere il modem "in pausa"** per fare una telefonata, per poi continuare la connessione Internet dal punto in cui ci si era fermati. Per poter sfruttare queste funzionalità, **è necessario che il proprio modem sia compatibile con lo standard V.92**; tutti i modem acquistati recentemente dovrebbero esserlo, e in molti casi **è possibile effettuare un aggiornamento del modem** scaricando un programmino dal sito del produttore.

Tutte le info su:
http://assistenza.tiscali.it/modem/v92/



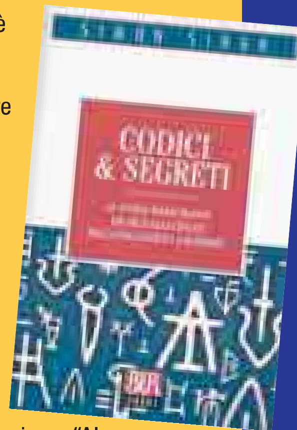
"HO GIRATO QUESTA NAZIONE IN LUNGO E IN LARGO, E HO PARLATO CON MOLTISSIME PERSONE IMPORTANTI. VI POSSO ASSICURARE CHE L'ELABORAZIONE DEI DATI È UNA MODA PASSEGGERA, CHE NON SOPRAVVIVERÀ FINO ALLA FINE DI QUEST'ANNO"

> Il caporedattore della collana di libri professionali Prentice Hall, 1957

HACKBOOK

CODICI & SEGRETI

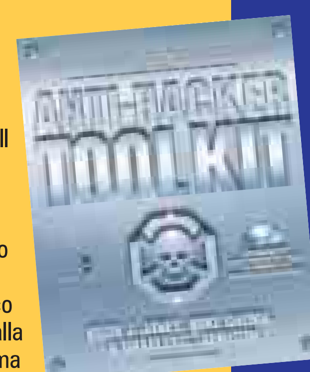
Autore: Simon Singh
ISBN:8817125393
Pagine:409
Prezzo: ¤ 8.80
Editore: Rizzoli, collana: BUR - Saggi LS



Il libro non è nuovo (è uscito nel 2000), ma merita senza dubbio una lettura. Ripercorre la storia della crittografia dagli antichi Egizi ai giorni nostri riuscendo a essere al contempo rigoroso sul lato tecnico, e affascinante e avvincente come un romanzo (cosa che non è da tutti...).
Come dice la presentazione: "Al centro di questo libro c'è l'ossessione di risolvere un rompicapo con le sole armi dell'intelligenza, e l'ossessione simmetrica di creare rompicapi che non si possano risolvere".

ANTI HACKER TOOLKIT

Autore: Keith Jones, Mike Shema, Bradley Johnson
ISBN:0072222824
Pagine:711
Prezzo:
Lingua: inglese
Editore: Mc Graw Hill



A parte il titolo, che dovrebbe essere "Anti Cracker Toolkit", il libro è ben fatto, e affronta con piglio molto pratico tutti gli aspetti legati alla protezione di un sistema informatico. In effetti, al teoria viene raramente affrontata senza avere anche un esempio pratico. L'edizione molto recente fa sì che il libro sia aggiornato sulle più nuove tecniche di intrusione. Oltre a trattare questioni relative alla sicurezza dei sistemi Unix e Windows, dedica parecchi risalto agli strumenti BSD.

HOT!

URGENZA AMERICANA

Un gruppo di consiglieri del presidente degli Stati Uniti ha appena approvato un rapporto che precisa **il carattere primario della scienza e della tecnologia nel campo della sicurezza nazionale**. Il gruppo di consiglieri noto con il nome di PCAST ha votato all'unanimità la presentazione al presidente di un rapporto dettagliato che lo informasse della necessità di attivare i militari, con lo scopo di **sbloccare i finanziamenti all'esercito per la cyber-guerra**.

AVIDO DI CUL-TURA!

Un giovane che nel 2001ha avuto la divertente idea di piratare in due riprese il sito Web di una biblioteca vicino a Filadelfia, negli Stati Uniti, è stato condannato a una pena da 1 a 3 anni di carcere e a una multa di € 15.000. Al suo primo passaggio **aveva sostituito la home page con una foto porno**, e con un'immagine a fumetti nel il secondo. Il sito ha dovuto essere chiuso per più di 3 settimane, quindi all'incirca 1 anno di carcere e € 5.000 per ogni settimana di chiusura.

LETTORI BLINDATI PER LE ANTEPRIME CD

I discografici sono stufi del fatto che, incuranti dei loro sforzi per pianificare le date di uscita dei nuovi album, alcuni malandrini spesso **distribuiscono su Internet tutte le novità prima ancora che i CD raggiungano gli scaffali dei negozi**. È abbastanza evidente che in molti casi a far filtrare i dischi siano **i redattori della stampa musicale, che ricevono i CD in anteprima** per la recenzione. Per questo, una divisione di Sony ha deciso di inviare ai giornalisti dei lettori Discman con dentro il CD in questione, ma **completamente inglobati nella colla, in modo che non sia possibile "ripparne" il contenuto** o collegare l'uscita cuffie a un registratore.

QUESTO FA MALE

Code Red è stato **il virus più devastante del 2001** con non meno di 300.000 calcolatori infettati (stima) e più di 3,1 miliardi di euro di danni! Gulp.

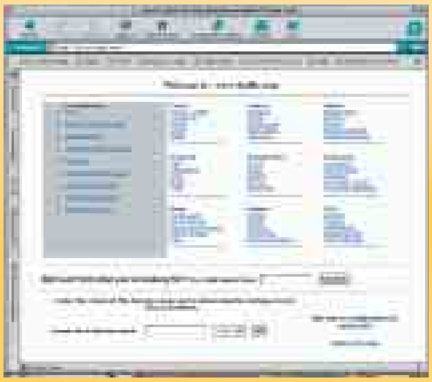
UNA SETTA "RAPISCE" UN SATELLITE CINESE

Dopo aver visto che la Cina moltiplica i suoi sforzi per modernizzare i suoi armamenti, ecco una notizia inquietante. Sembra che durante i mondiali di calcio, **un satellite di una catena televisiva cinese sia stato violato da pirati informatici**. Con ogni probabilità, il responsabile sarebbe la setta Falun Gong. Le vittime dirette di questa pirateria sono state limitate, perché il satellite consentiva la diffusione dei mondiali tra il 23 e il 30 giugno in certe zone rurali della Cina. I danni avrebbero potuto essere di ben altra portata se l'obiettivo fosse stato un satellite diretto a un pubblico più numeroso. Il ministero dell'informazione e delle comunicazioni cinese ha confermato questa informazione e ha precisato che la pirateria di 9 canali della cinese CCTV (China Central Television Station, stazione televisiva cinese centrale) e di 10 canali televisivi locali è stata commessa sotto l'egida di Li Hongzi, il capo spirituale della setta Falun Gong. I programmi, qualcuno dice, sono stati sensibilmente disturbati per una settimana, e questo costituisce un grave attentato secondo la legislazione cinese. **I contenuti pirata diffusi occasionalmente erano propaganda della setta Falun Gong**. Dopo un breve periodo durante il quale gli schermi sono rimasti oscurati, sono arrivate ai televisori dei contadini cinesi emissioni intermittenti con immagini di meduse.



TRUFFA.COM

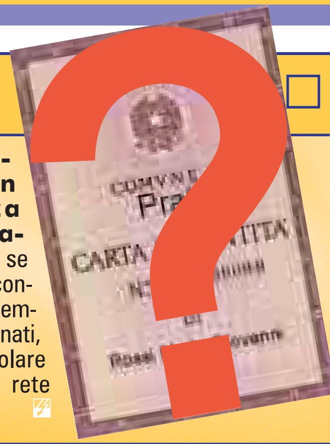
Una grossa operazione condotta dall'FBI ha permesso di porre fine a tutta una serie di truffe e furti online. Non meno di 19 persone sono state interrogate. Una delle truffe, Stuffingforcash.com, **prometteva alla gente più di 2.000 euro alla settimana per ricevere buste a casa**, avendo come sola condizione un diritto di iscrizione di 45 euro.



Unico inconveniente, una volta pagata l'iscrizione non si ricevevano più notizie. Questa truffa sembra avere fruttato più di 2 milioni agli organizzatori… Qui da noi, **analoghe truffe vengono perpetrate quotidianamente attraverso le inserzioni dedicate alla ricerca di personale** su riviste e quotidiani, ma gli autori raramente vengono arrestati (e questo nonostante alcune inchieste giornalistiche li abbiano spesso smascherati).

NEWS

DOCUMENTI PREGO...



Il furto o usurpazione di identità è senza dubbio una delle attività criminali più sviluppate negli Stati Uniti, ma nonostante ciò l'e-commerce non si lascia intimidire e i consumatori non moderano i loro entusiasmi. Dei 7,2 miliardi di dollari generati dall'e-commerce nel 2002, **gli acquisti effettuati con usurpazione di identità non rappresentano che una goccia nell'oceano**. Questo è almeno ciò che afferma l'istituto Forrester. Ma questa pratica aumenta **senza che si arrivi a identificare con esattezza gli usurpatori**, anche se i metodi di controllo sono sempre più raffinati, in particolare grazie alla rete Internet...!

ARABIA SAUDITA: CENSURA DI MASSA



Se da Riyad proviamo a collegarci per esempio al sito Internet dei Rolling Stones o al nostro sito Web personale ospitato da Geocities, rischiamo di avere una grossa delusione: **questi indirizzi fanno parte dei 2.000 siti Web bloccati dal governo arabo per "preservare i valori dell'Islam"**. Una situazione che arriva fino all'impossibilità di accedere al sito Web della Warner Bros... Contrariamente a quanto si crede, **l'Arabia Saudita è uno tra gli stati che applicano le più severe restrizioni di tipo religioso**, principalmente sulle donne; un regime duro ma **sostenuto da tutte le democrazie occidentali** in spregio ai diritti umani. Solo pochi paesi limitano l'accesso a Internet dei cittadini: Vietnam, Cina ed Emirati Arabi Uniti.

I MILITARI LAVORANO A CARTE DI IDENTITÀ HIGH TECH



La biometria acquista una nuova dimensione con le nuove carte di identità destinate ai militari americani: impronte digitali, ma anche altre caratteristiche fisiche. Le nuove carte contengono **il nome, una serie di numeri e una foto del proprietario** e ne è già stato codificato più di un milione. Da qui al 2007, esisteranno più di tre milioni di queste carte per i dipendenti del Pentagono. I possessori potranno essere tracciati in tutti gli spostamenti all'interno dei locali dell'esercito.

STUDENTI PER COMBATTERE IL CYBER CRIMINE

Alcuni studenti dell'università di Tulsa in Oklahoma hanno accettato un **accordo con la polizia per lottare contro la cyber criminalità**. Da qualche settimana i poliziotti si sono installati in nuovi uffici in seno all'università. Gli oggetti delle indagini sono principalmente **pedofilia, truffa, pornografia e altri simili reati**. L'obiettivo degli studenti è chiaro: si tratta di approfittare di questo accordo per ottenere una certa esperienza sul terreno in materia di sicurezza informatica.

Tutti gli studenti di informatica sono volontari, ma non saranno portati a testimoniare davanti a una corte di giustizia, anche se il loro intervento in un'inchiesta dovesse implicare una testimonianza. Un piccolo spirito delatorio che non farà male a nessuno?

HOT!

FINANZIAMENTI CONTRO IL CYBER TERRORISMO

Due università americane hanno appena ottenuto un finanziamento record da 6,4 milioni di dollari da parte del governo federale americano per effettuare ricerche e formare i responsabili per il governo e per l'industria dei mezzi di protezione delle reti informatiche contro gli attacchi.

HP VOLEVA CENSURARE LA CRITICA

Alcuni non amano la critica. È il caso di HP che ha minacciato di conseguenze un ricercatore, prima di ritirare la sua accusa. Questo, con lo pseudonimo di Phaser, ha pubblicato ciò che gli hacker chiamano solitamente un "exploit". Ha dimostrato molto semplicemente la vulnerabilità agli attacchi pirata del sistema Tru64 Unix di cui lo sviluppatore ed editore non è altri che HP. HP non ha affatto apprezzato...

OLANDA, IL PAESE DELL'INDISCREZIONE

Un fornitore di accesso a Internet per errore ha inondato di e-mail un vecchio cliente. Il problema è che i messaggi contenevano dati privati e confidenziali di file di clienti del provider. Tutta la storia è cominciata quando il cliente ha voluto interrompere il suo abbonamento con l'operatore Casema. Invece di vedere eliminati i suoi privilegi, il cliente ha ricevuto messaggi contenenti informazioni bancarie di altri clienti! Niente male come gaffe!

"NON VEDO VANTAGGIO ALCUNO NELL'UTILIZZO UN'INTERFACCIA GRAFICA"

> **Bill Gates, 1983**

mailto:
redazione@hackerjournal.it

FANGO SULLA RETE

Non ho fatto in tempo a leggere e rimuginare sul vostro editoriale del numero 7 riguardante i mostri presunti della rete, che ci si imbatte nell'omicidio di Torino: coppia torna dalle vacanze e trova la figlia strangolata! Presunti colpevoli o sospetti i 5 con cui la poverina chattava in rete. Poi viene arrestato il fidanzato che con internet e PC non c'entrava per un bel niente... intanto il tam-tam dei giorni scorsi sui pericoli della rete si era rimesso in moto.

LED

Tranquillo: qualche TG non ha esitato a far notare che anche il fidanzato aveva conosciuto Nadia via Internet. Due anni prima. Il capro espiatorio è sempre valido.

REATI SATELLITARI

Essendo patito non solo d'informatica, ma anche di telecomunicazioni mi sono avvicinato al mondo delle trasmissioni satellitari. Non nego che mi sono fatto tentare dai vari (ex) codicini presenti in rete e provarli. Certo ciò non è legale, ma l'obiettivo primario era per scopo di studio, e mi sono addentrato sempre più nello studio di questo tipo di trasmissione. Ora, con la nuova codifica (Seca2) tutti sono fuori (meno male), o quasi. Infatti da due mesi a questa parte, sembra sia uscita una scatoletta (attualmente in fase di test personale) che promette la visione in chiaro di tutti i canali. Ora con questa, non c'è bisogno ne di modificare decoder, o cam o schedina sim, infatti viene montata tra parabola e decoder. Insomma,



Kernel Panic immagina un Mozilla che bruci Internet Explorer, e con un po' di creatività e qualche pezzo di software la fantasia può diventare realtà, almeno in un'immagine.

Professori da bocciare

Ho deciso di scrivervi dopo aver letto (a pag. 2 del n. 7) la lettera di Francesco, che lamentava l'ignoranza dei suoi professori. Sono un insegnante anch'io e sono perfettamente d'accordo con lui per quanto riguarda il livello di preparazione dei docenti, che non di rado è poco elevato. Conosco insegnanti di materie specifiche (laboratorio di informatica e trattamento testi) che non sanno nemmeno -lo giuro!- come nascondere la barra di Windows. Nonostante lo stipendio di un insegnante sia quanto meno dignitoso (non dimentichiamo che la commessa del supermercato guadagna molto di meno e lavora molto di più) ben poco spendono, non dico per i libri, ma addirittura per l'acquisto di riviste o per un non meglio precisato (ma significativamente sbandierato) "aggiornamento" che dovrebbe rappresentare il fiore all'occhiello di un lavoratore nel campo educativo. Non parliamo poi degli investimenti in hardware e software. Eppure, se guardiamo le spese per aggiornamenti professionali di docenti e l'installazione di laboratori di informatica, centinaia di migliaia di euro compaiono nelle spese dei bilanci di scuole e istituti secondari. Sicuramente molti colleghi reagiranno violentemente a queste mie parole: ma basterebbero poche considerazioni per far rientrare la protesta. Sarebbe sufficiente che ognuno di loro segnasse il numero di ore mensili dedicate all' aggiornamento professionale, oppure indicasse le cifre spese annualmente nel medesimo campo. Oppure si potrebbe proporre di sottoporli a un esame serio sulle loro competenze, esame in cui l'esaminatore fosse Francesco o qualunque altro studente che -vi assicuro che ve ne sono- ne sanno molto di più di certi prof. Il problema è che un insegnante, una volta immesso in ruolo, non viene mai più sottoposto a verifica. In passato ho partecipato a corsi di aggiornamento, al termine dei quali rilasciavano l'attestato senza sottopormi ad alcun esame. In altri casi, l' attestato viene rilasciato consegnando agli esaminatori una "ricerca", senza metterne in dubbio la paternità. Ed ecco che alla fine la Scuola pullula di insegnanti "certificati", che però possono essere messi alla berlina da qualunque studente come Francesco, che ha il grande vantaggio di possedere e manifestare quell'onesto entusiasmo che è alla base della Conoscenza e della Cultura con la "C" maiuscola.



Alessandro

Saremo di nuovo in edicola Giovedì 10 Ottobre!

STAMPA LIBERA NO PUBBLICITÀ SOLO INFORMAZIONI E ARTICOLI

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

Problemi di posta

Non riesco ad entrare nella mia casella di posta elettronica (@hackerjournal.it) anche seguendo alla lettera le vostre indicazioni... e immettendo la password da voi recapitatami. Fate questa ispezione!!

Saimon

Tieni presente che come nome utente devi usare tutto l'indirizzo (cioè "nomeutente@hackerjournal.it" e non semplicemente "nomeutente").

Quando ho sottoscritto l'account con voi non mi è stato comunicato quale fosse il server della posta in uscita (smpt). E poi, se non sbaglio, solo Outlook Express supporta il server http del vostro account: non va contro i vostri principi favorire lo zio Bill?

Tofu107

Come Smtp devi usare quello che usi normalmente (probabilmente, quello del tuo provider). La posta può essere scaricata dalla casella con qualsiasi client Pop3, oppure letta dal Web con qualsiasi browser. Forse ti confondi col fatto che Outlook scarica in Http la posta di Hotmail.

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: 7mbre
pass: sen6

GLI SFONDI SCRIVANIA DI HACKER JORUNAL!

Da oggi puoi avere le splendide copertine di Hacker Journal sullo sfondo del tuo computer. Basta che ti colleghi a www.hackerjournal.it/secretzone, inserisci il nome utente e la password che trovi qui a sinistra, e potrai scaricare lo sfondo nel formato che preferisci (800x600 o 1280x1024). Occhio perché i codici cambiano con ogni uscita della rivista.















se dovesse funzionare, si vede tutto senza modificare nulla. La mia domanda è: se non tocco decoder, cam o scheda, dato che è una cosa che si monta dopo la parabola (antenna) si incorre in qualche sanzione penale? e se si che tipo di sanzione, dato che non si toccano le parti elettriche (decoder cam e sk).

Bit

Allo stato attuale, l'uso di sistemi per la cosiddetta "pirateria satellitare" non è previsto come reato penale. È in discussione una legge che cambierà questo stato di cose, ma per il momento, nessuno può metterti in galera perché hai una card pirata. Discorso diverso per chi invece gli apparecchi li vende, che per di più solitamente vendono le schede "in nero".

GUIDA PYTHON IN ITALIANO

Ho letto in "Come diventare un hacker" che Eric S. Raymond consiglia il Python come linguaggio per chi si avvicina al mondo della programmazione. Dove posso trovare guide e informazioni in Italiano?

Guido

Facile... www.python.it. Tutte le info esistenti in italiano sono lì. Comunque, imparare bene l'inglese è fondamentale per chi vuole rimanere aggiornato sulle materie tecniche. Pensaci.

VISUAL BASIC WINSOCK

Sul numero 6 di agosto c'è un articolo sulla sicurezza che spiega come creare un programma di ascolto sulle varie porte del PC. Non riesco a trovare tra gli oggetti di VB "Winsock".

Vito

Nella finestra principale di VB premi control-T, oppure scegli Componenti dal menu Progetto e da qui selezioni Microsoft Winsock Control.



"Vi invio un mio disegno riguardante il mio pensiero su HackerJournal" (Jabbo8)

GLI MP3 NON SONO ILLEGALI

Ho appena letto l'articolo a pag.12 dell'ultimo numero (quello dove si parla del fatto che la Riaa vuole poter hackerare le reti Peer2Peer per trovare chi ha Mp3 copiati), e volevo chiedervi se quindi allora sarà pericoloso anche a noi italiani prelevare mp3 dalle reti tipo Open Nap, Gnutella...

AKKI84

In Italia non è vietato avere musica non originale: è vietato solo venderla. Del resto, tutti noi paghiamo un contributo su ogni CD vergine per garantirci l'utilizzo personale... Comunque, sarebbe una cosa carina ricompensare giustamente gli autori che ti piacciono tanto (magari andando ai loro concerti, dai quali guadagnano molto di più che dalla vendita dei dischi, il cui ricavato viene intascato quasi per intero dai produttori).

CASELLA INFESTATA

Da alcune settimana ricevo sul mio indirizzo di posta elettronica principale fino a 3 mail con allegato il virus w.32KLEZ.
Regolarmente il mio antivirus le intercetta ed elimina,ma ovviamente la situazione è di disagio! Ma il punto è che io non ho mai rilasciato quell'indirizzo su alcun sito,secondo voi allora com'è possibile questo attacco?
Le mail hanno tutte indirizzi diversi quindi è inutile bloccare i mittenti,che mi consigliate? Devo abbandonare l'indirizzo? Posso segnalare la cosa al provider, ma dubito possa essermi d'aiuto.

Fabrizio

Non ti dico quante ne riceviamo sulle caselle della redazione...
C'è poco da fare, se non evitare di usare Microsoft Outlook e stimolare i propri amici a fare altrettanto: indipendentemente dai mittenti che vedi indicati, i messaggi arrivano da persone che usano Outlook e hanno il tuo nome nella loro rubrica.

SPIE DILETTANTI ALLO SBARAGLIO

È vero che anche senza essere in possesso dei Tabulati Telecom è possibile sapere le generalità (nome e cognome) sapendo solo l'indirizzo IP???
Io credevo che solo la Polizia potesse farlo ma vorrei chiedervi conferma.

..:: MiKiSpAg ::..

La seconda che hai detto. Solo le Forze dell'Ordine possono rintracciare una persona dall'IP della sua macchina. Questo se, come si intuisce dalla tua mail, la connessione avviene attraverso una linea telefonica. Discorso diverso per chi ha una connessione dedicata, con IP fisso e un nome a dominio. In quel caso, attraverso il database Whois della Registration Authority (www.nic.it/RA/database/viaWhois.html) puoi effettivamente ottenere informazioni anagrafiche, ma solo su chi ha registrato il dominio e del responsabile tecnico.

TROJAN O NO?

Masterizzando un cd con Nero Burning Rom, ho spuntato l'op-

04_07_HJ09_posta 18/09/2002 16:56 Pagina 7

Saremo di nuovo in edicola Giovedì 10 ottobre

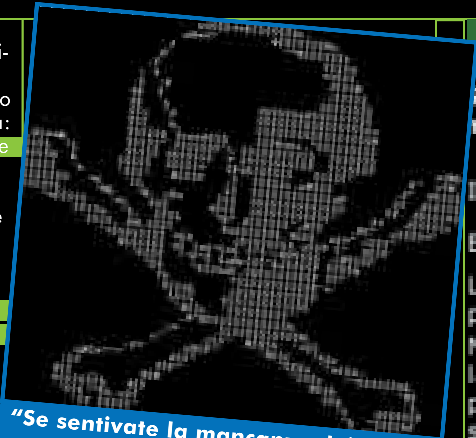
STAMPA LIBERA NO PUBBLICITÀ SOLO INFORMAZIONI E ARTICOLI

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

zione "Effettua un controllo virus prima della scrittura".
Una volta finita la scansione di Nero è apparsa una finestra con la scritta: Nero ha rilevato che il seguente file è forse infetto... Nome virus: Trojan.Slider
Il file in questione è un .exe che scompone il desktop in caselle da sistemare e che ho scaricato da internet, il nome è "Hot as a Fire". Allora ho provato a scansire il file con Norton 2002, ma non è stato rilevato nessun virus o trojan, da precisare che ho controllato l'elenco dei nomi dei virus di Norton e questo nome non c'è.
Non sapendo cosa fare ho eliminato il file sperando che così venga eliminato anche il trojan.
Ti prego di darmi qualche spiegazione in merito, e se la procedura per eliminare il trojan è giusta.

Giuliano G.

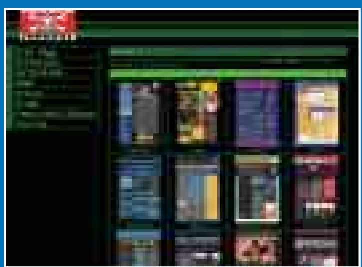
Prova a usare un rilevatore di trojan (vai su www.download.com e cerca i programmi che contengono Trojan...). Se trovi un file infetto ma non rilevato dall'antivirus che usi, in genere puoi mandarlo ai produttori del programma, che lo analizzeranno per includere la protezione antivirus specifica nel successivo aggiornamento.
Nel tuo caso, che usi Norton AntiVirus, puoi mandare il file sospetto con le modalità descritte all'indirizzo http://securityresponse.symantec.com/avcenter/submit.html
PS: ovviamente do per scontato che l'antivirus lo hai aggiornato, vero?



"Se sentivate la mancanza dei teschi, eccovene uno in Ascii..." (Renato C.)

Arretrati e abbonamenti

Siete in tanti a chiederci se sia possibile abbonarsi o richiedere i numeri arretrati di Hacker Journal, che ormai stanno diventando oggetti da collezione. Stiamo cercando di allestire le strutture necessarie, ma potrebbe essere necessario un po' di tempo. Intanto, potete trovare i PDF di tutti i vecchi numeri sul sito nella Secret Zone, e già che siete sul sito, iscrivetevi alla nostra mailing list: sarete avvisati non appena i servizi abbonamenti e arretrati saranno disponibili.



IL GIOCO È BELLO QUANDO CONTINUA

Ho visto che è finita la sfida di try2hack, vorrei x questo segnalarvi un link chiamato LoginMatrix, non so se lo conoscete ma sappiate che la sfida non può finire....
Ecco il link del gioco www.loginmatrix.com/hackme/

Chris

La sfida finisce solo quando lo decidi tu... La vera sfida è con te stesso, e non serve ad apparire in una classifica (anche se fica come la nostra). Non è mica obbligatorio leggere le soluzioni che abbiamo pubblicato sul numero scorso ;-) Comunque grazie per il link: lo visiteremo al più presto.

Sondaggio

Secondo te, chi spia le tue navigazioni e le tue email?

Il mio provider	44.1%
Echelon	35.0%
Le forze di polizia	13.7%
Nessuno: uso la crittografia per ogni scambio di dati sensibili.	7.2%

Voti Totali: 1435

Questa volta ci avete un po' sorpreso: la maggior parte di voi ha la sensazione che il proprio provider "spii" il contenuto delle email e le navigazioni dei suoi utenti. In effetti, sarebbe tecnicamente molto facile intercettare ogni comunicazione "alla fonte", e un provider potrebbe trovare in questi dati informazioni utili alle sue campagne pubblicitarie. Da qui a ipotizzare un monitoraggio di massa, francamente ce ne passa. Però, vedendo quanto è sentito questo argomento, potrebbe essere il caso di passare la parola ai provider, per farci raccontare quali sono le loro politiche per la tutela della privacy dei propri utenti: vi faremo sapere.
In seconda posizione, ma molto vicino al primo posto, troviamo Echelon, il sistema messo a punto da americani, inglesi e neozelandesi per monitorare tutte le comunicazioni che avvengono in modo digitale, e del quale non si riescono ad avere informazioni precise e ufficiali.
Curioso notare che la risposta più ovvia (e più giustificata), le Forze dell'Ordine, si piazza molto in basso nella classifica: troppo banale forse? Solo il 7 per cento dei lettori poi se sente tranquillo perché sostiene di utilizzare sistemi di crittografia per ogni scambio di informazioni riservate, una percentuale che –seppur interessante– è ancora lontana da un'utilizzo di massa della crittografia, unica vera garanzia di riservatezza nel mondo delle informazioni digitali.

QUESTO SPAZIO È VOSTRO!
APPROFITTATENE, E FATE LAVORARE QUELLA TASTIERA!

Saremo di nuovo in edicola Giovedì 10 Ottobre!



Farsi cattiva pubblicità

A volte con lo scopo di promuovere le proprie idee si rischia di farsi cattiva pubblicità. È quello che ormai stanno facendo alcuni sedicenti hackers e sostenitori Linux.
A sostenere la tesi vi porto la mia diretta testimonianza.
Premetto che io sono un utente, che per necessita' di lavoro e di studio, ha installato una mini-rete composta da tre postazioni. Su due di queste macchine gira un sistema Linux, mentre sulla terza Win98.
Ovviamente non tutti a casa mia sono "aperti" a imparare il pinguino, per cui utilizzano regolarmente il Win-PC. Circa una settimana fa', ho formattato proprio quest'ultimo computer e, reinstallato Windowz, ho cominciato a inserirvi solo le applicazioni essenziali che normalmente una postazione deve avere: antivirus, firewall, Office e una zip-utility. Proprio quest'ultima mi ha fatto capire quanto stronXe siano alcune persone.
Trovato un programmino freeware su una nota rivista, e valutando come questa applicazione mi permettesse di gestire un sacco di formati (compresi quelli caratteristici di *nix), ho provveduto subito ad installarlo dicendomi: "Un buon programma legalmente fruibile! GRAZIE".
Dopo 2 giorni, senza che nulla di nuovo fosse aggiunto al PC, mi appare durante l'avvio un messaggio d'errore. Ad essere strano era quel simbolo triangolare e giallo: non era circolare e rosso! Non proseguendo la procedura d'avvio, premo ALT+F4 pensando ad un normale scherzo, ma mi appare una seconda form con scritto: "Linux is better then Bill's s.o. . Only stupids use Winzozz!"... E in più il sitema risultava bloccato!
Reinstallo Win98 e tutto torna a funzionare.
Mi collego ad internet per vedere se qualcosa di simile è successo ad altri (ed è percio' documentato); ma passando per la home-page della ditta per cui lavoro mi fermo: scopro esservi una bella DefacedHomePage. L'azienda produce software per vari sistemi operativi, quasi tutti freeware (non sto facendo pubblicità :), e vive quasi esclusivamente di assistenza ai clienti. Cosa fa di male per vedersi rovinare il suo sito, unica forma di pubblicità? Defacciare non è da hacker! È semplice e stupido se lo si fa con un normale bruteforce sulla porta 21, conoscendo solo lo username (presente sugli indirizzi mail...)!
Al mio fianco è sempre rimasta la mia ragazza, la quale usa il computer come un utente medio, e non ha nessuna intenzione di alzare il suo livello. Ultimamente l'avevo convinta ad avvicinarsi al pinguino col cappello rosso, insegnandole a montare e smontare un filesystem da shell. Dopo quello che ha visto, ora crede che Linux sia territorio esclusivo per dei nerd che non hanno un cazzo da fare se non rompere le palle, e che gli hacker siano degli stronzi con il gusto di fare danni agli altri solo per sentirsi grandi. Così la pensano tanti altri utenti che preferiscono la semplicità dei sistemi di zio Bill, alla serietà e solidità di sistemi unix-like.
Siamo onesti: anche Linux ha i suoi limiti. Lo so bene io che ho sudato sette camice per far partire un winmodem, solo perché mal supportato dalla mia distribuzione: almeno Win non fa difficoltà sulla periferica! e oltre a questo posso aggiungere mille e mille altri esempi!
Credo che grazie a questa mia giornata nera, Bill abbia solidificato il rapporto con un cliente che stava per migrare, e RedHat abbia perduto un aspirante utente.
Grazie della pubblicita' che ci fate facendo simili idiozie. Grazie anche da parte di Bill Gatto :(

LOXEO

UN GIORNALE PER TUTTI: SIETE NEWBIE O VERI HACKERS?

NEWBIE
MID HACKING
HARD HACKING

Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere di hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un level: NEWBIE (per chi comincia), MIDHACKING (per chi c'è già dentro) e HARDHACKING (per chi mangia pane e worm).

HJ ha surfato per voi...

Il meglio della rete



www.sikurezza.org

Home page di alcune mailing list italiane dedicate alla sicurezza informatica. Ospita le informazioni su come iscriversi alle mailing list e gli archivi dei messaggi delle liste. In particolare, crypto@sikurezza.org è dedicata alla crittografia (algoritmi, teoria, pratica...). Come il nome lascia intendere, openbsd@sikurezza.org è una lista per gli utenti del sistema operativo OpenBSD (www.openbsd.org). C'è anche la lista del Progetto Angel (angel@sikurezza.org), un modulo per il kernel Linux nato con lo scopo di bloccare gli attacchi informatici.



www.html.it

Uno sei siti storici della Rete italiana, Html.it è partito come punto di riferimento per i Webmaster in erba, e ora affronta tantissimi argomenti legati all'informatica in generale, e alla programmazione in particolare. Molto utili le Guida (di base e avanzate) sugli argomenti e i linguaggi più disparati. Per i Webmaster poi ci sono i Webtool: risorse varie da aggiungere al proprio sito, dai contatori alle statistiche, dai sondaggi allo scambio di banner.

15 MINUTI DI CELEBRITÀ! QUESTI SONO I VOSTRI



www.extrhack.da.ru

L'idea di realizzare un portale hacker italiano, è nata nel 2000 con il primo progetto intitolato ItAck. Oggi ExtrHack fa un ulteriore passo in avanti, unendosi al progetto di "FaiPure", crew nata da un canaleirc. I membri sono un gruppo di amici con gli stessi interessi: rendere sicuro il mondo della rete e combattere per una cultura libera. Il nostro motto? Il sapere è un diritto di tutti... Se non ce lo date ce lo prenderemo!!!

itack



www.electronicdream.it

Vi Segnalo il nostro sito; ci interessiamo di sicurezza, elettronica e programmazione... tutto ciò che per noi è hacking! È aperto da poco ma stiamo preparando molte sorprese!!!

MaiN...



www.tuttoscript.net

Oltre a farvi i meritati complimenti per l rivista volevo segnalarvi il nostro sito dedicato a Mirc e irc, ci sono recensioni, tutorial e parecchio altro materiale.

ToOLaMaH

Segnalate i vostri siti a: redazione@hackerjournal.it

SITI; SCEGLIETE VOI SE TIRARVELA O VERGOGNARVI

Il meglio della rete

www.mojodo.it



Sono un membro del mojodo project, un gruppo di ragazzi che si interessano di sicurezza, programmazione e open source. Vi scrivo per chiedere di inserire il nostro sito ,dove potrete trovare lezioni di programmazione, articoli interessanti, forum e molto altro.



http://hacking123.supereva.it

Vorrei che pubblicaste il mio sito hacker. È è ricco di sezioni, programmi e soprattutto guide!!!! Buon lavoro e complimenti per le illustrazioni in copertina!

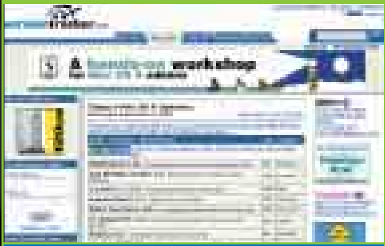
hacking123



www.programmo.net

Vi volevo segnalare il mio sito, dedicato alla programmazione Questo sito è dedicato interamente alla programmazione in C, C++ e Visual C++. Penso di estendere questo sito su altri linguaggi di programmazione e perciò, se qualche lettore fosse interessato, sarò ben lieto di affidarglli la gestione di nuove sezioni.

Meox



www.versiontracker.com

Qualsiasi utente Mac di buon senso, dovrebbe avere tra i bookmark un solo indirizzo per tutto quello che riguarda il download di programmi: Versiontracker. Qui vengono riportati in un'unica e pratica pagina tutti i nuovi programmi e gli aggiornamenti usciti nell'arco della giornata (e sono tanti!). Ogni programma ha una scheda di descrizione e degli utilissimi commenti degli altri utenti. In realtà esistono anche una versione Windows e una per Palm (raggiungibili dalla home page), ma bisogna dire che ancora devono crescere per arrivare al ritmo di aggiornamento della versione Mac.



www.1minutesite.com

Cosa c'entra con Hacker Journal un libro che parla di siti per le piccole e medie aziende? C'entra, c'entra, perché a giudicare da quello che vediamo, alcuni dei vostri siti avrebbero bisogno di una cura dimagrante simile a quella proposta dal duo Oliva&Toscani: meno orpelli e più comunicazione. Il libro, scaricabile gratuitamente in formato Pdf, si legge tutto d'un fiato. A voi non resta altro che sostituire Pmi (piccola e media impresa) con Crew, clienti con membri, e il gioco è fatto.



CACCIA AI PIRATI DEL SOFTWARE

QUALSIASI CONTROLLO DA PARTE DELLE FORZE DELL'ORDINE PUÒ METTERE UN PO' A DISAGIO I CITTADINI ONESTI NON ABITUATI AD AVERE A CHE FARE CON LA LEGGE. HJ VA "A LETTO COL NEMICO", E INTERVISTA PER VOI UNO CHE DELLA CACCIA AI PIRATI HA FATTO UNA PROFESSIONE: ENZO BORRI

PIRATERIA INFORMATICA: COME TUTELARSI IN CASO DI CONTROLLI?

I controlli dell Forze dell'Ordine in materia di pirateria informatica sono sempre più frequenti. Come tutelarsi e come essere pronti nel caso ci trovi sottoposti a un controllo?
Ne parliamo con Enzo Borri, che è un consulente antipirateria informatica per alcune aziende e ha partecipato in qualità di Ausiliario di Polizia Giudiziaria in occasione di numerosi controlli antipirateria.

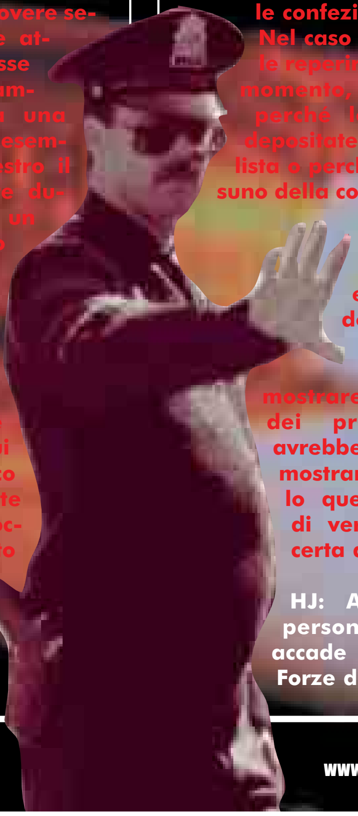
Hacker Journal: In genere un controllo delle Forze dell'Ordine, può "bloccare" una società per parecchio tempo?
Enzo Borri: No, i controlli sono molto rapidi –qualche minuto per ciascun PC– e solitamente non causano disagio all'azienda o interruzione delle attività.

HJ: Come si dovrebbe comportare un'azienda?
EB: Le cose fondamentali da fare in caso di controllo sono: indicare quanti e dove sono ubicati gli elaboratori e consentire il relativo accesso; individuare una persona che segua passo passo le operazioni di controllo (meglio se il tecnico di fiducia o una persona che conosca il parco software); recuperare tutta la documentazione attestante il regolare possesso dei programmi (fatture e confezioni originali). Se si dispone di un elenco del software, meglio se accompagnato dalla documentazione contabile, è buona norma (e fa anche un'ottima impressione) mostrare subito questo materiale.

HJ: A proposito di "dare un'ottima impressione": cosa bisogna evitare di fare?
EB: Assolutamente non cancellare nulla! Vista la semplicità con cui si può scoprire che alcuni programmi sono stati da poco cancellati, si rischia solo di trovarsi in una posizione ben più scomoda, dal punto di vista legale, rispetto alla semplice presenza di un programma copiato!

HJ: C'è modo di tutelarsi per evitare abusi?
EB: Devo dire con estrema sincerità che ho sempre visto agenti operare nel massimo rispetto e con la massima correttezza, quindi il rischio è praticamente nullo. Nel caso comunque si pensi che vi siano delle irregolarità relative alle procedure di controllo, ci si può rivolgere al "Garante per i diritti del contribuente". Le sedi sono presenti in tutte le

14_16_hj09_borri2 18/09/2002 17:01 Pagina 15



regioni e i relativi recapiti sono disponibili su www.garantedelcontribuente.it.

HJ: E se non fossero Agenti?
EB: La prima cosa che un agente fa nel presentarsi, è mostrare il proprio tesserino di riconoscimento. Se vi fossero dei dubbi sulla sua identità, si può telefonare alla caserma da cui dipendono gli agenti (di solito sono in due o più), verificando i dati.

HJ: Si sa che in molti casi, per non sbagliarsi, le Forze dell'Ordine sequestrano tutto il materiale informatico presente (a volte persino le stampanti!). C'è modo per minimizzare le apparecchiature sequestrate?
EB: Nei casi in cui ho assistito ho potuto constatare che le Forze dell'Ordine hanno una ottima preparazione. Per interrompere la continuazione del reato, gli agenti possono scegliere vari sistemi alternativi poco dannosi per la società, senza dovere sequestrare e asportare attrezzature. Se si trattasse di bloccare dei programmi copiati in uso a una azienda, possono per esempio porre sotto sequestro il materiale illecitamente duplicato inserendolo in un archivio compresso protetto con password.

HJ: Entriamo nel vivo: come avviene di solito il controllo?
EB: Generalmente vi è una prima fase in cui vene redatto un elenco del software presente sugli elaboratori. Ad occuparsi del rilevamento di quanto installato di solito è un tecnico nominato Ausiliario di Polizia Giudiziaria. Egli esaminerà la presenza di programmi sull'elaboratore e redigerà l'elenco. Questo viene fatto sempre in presenza della persona incaircata dall'azienda, che verificherà che non vengano esaminati documenti personali o aziendali, che non vengano arrecati danni al materiale informatico ma che siano esaminati solo ed esclusivamente i programmi. In caso di controlli fiscali, l'ausiliario di P.G. potrebbe essere incaricato di aprire i documenti rinvenuti al fine di consentire o agevolare la verifica fiscale.
La seconda fase del controllo consiste nella verifica del materiale fornito, per attestare il regolare possesso dei vari programmi rinvenuti durante la prima fase. Ecco il motivo per cui si consiglia vivamente di conservare –archiviandole a parte– copie delle fatture di acquisto dei prodotti software e quant'altro sia utile a dimostrarne il regolare possesso (per esempio i CD o le confezioni originali).
Nel caso non sia possibile reperire il materiale al momento, per esempio perché le fatture sono depositate dal commercialista o perché non vi è nessuno della contabilità reperibile, può essere utile chiedere di potere esibire questi documenti in un secondo tempo. In questo caso il mostrare le confezioni dei programmi non avrebbe la validità del mostrare le fatture; solo queste consentono di verificare la data certa di acquisto.

HJ: A proposito di personale ausiliario: accade a volte che le Forze dell'Ordine siano accompagnate da personale della BSA (Business Software Alliance, l'associazione antipirateria dei maggiori produttori software). Non è un po' strano questo?
EB: Non trovo nulla di strano. Credo sia normale per le Forze dell'Ordine rivolgersi a chi ha esperienza tecnica e competenza in materia di antipirateria. Va detto anche che quando si opera come Ausiliare di P.G. la cosa più importante è agire in modo sempre corretto e obiettivo viste le responsabilità affidate.

HJ: Una volta fatta la verifica, che succede?
EB: Se tutto è risultato regolare verrà redatto un verbale con esito negativo. In questo caso, non vi è null'altro da fare che archiviare questo verbale e complimentarsi con sé stessi!
In caso di controllo positivo, le cose sono meno allegre. Infatti il reato per i quali viene sporta denuncia, è un reato penale. È quindi suggeribile rivolgersi a un buon avvocato. È fondamentale affidarsi a un legale esperto di diritto d'autore. La materia – soprattutto in campo informatico – è piuttosto nuova quindi, nel proprio interesse, è meglio affidarsi solo a professionisti con una preparazione specifica in questo settore.

HJ: Quali sono quindi i tuoi consigli per chi vuole stare tranquillo?
EB: Oltre all'avere software originale, occorre poterlo dimostrare; meglio se in tempi brevi. A questo scopo è buona norma tenere sempre a portata di mano un elenco del software installato per ciascuna postazione. Conservare sempre le fotocopie dei documenti attestanti il regolare possesso. In caso di acquisto di programmi abbinati a componenti hardware o a computer, verificare che nella fattura sia sempre elencato tutto il software fornito

PIRATERIA INFORMATICA: COME TUTELARSI IN CASO DI CONTROLLI?



a corredo. Alcuni elaboratori hanno CD forniti dalla casa contenenti antivirus e altri programmi; la maggior parte dei computer viene fornita di sistema operativo e così via. Assicurarsi quindi che la fattura riporti tutti i dettagli quali nome del programma, produttore e versione. Nel caso non sia così, si può richiedere al rivenditore una distinta di quanto acquistato oppure estrarre dai supporti dati contenenti il software a corredo un elenco da conservarsi assieme al supporto dati. Potrebbe infatti accadere che un sistema operativo o dei programmi forniti a corredo con un computer come "precaricati" siano forniti in modo assolutamente regolare ma senza CD o manuali. È il caso dei sistemi operativi che sfruttano una parte di disco rigido come "disco di ripristino". In questi casi, se non vi è materiale attestante il regolare possesso (indicazione in fattura, CD originale o manuali), sarebbe arduo dimostrare la propria regolarità!
Conviene sempre verificare quanto consentito dalla Licenza d'uso. Infatti, se venisse contestato che un programma è installato su un elaboratore fisso e su un portatile, entrambi in uso alla medesima persona, conviene verificare la licenza: molti produttori consentono questa pratica. Questa è una cosa che poche persone sanno. Per chi assiste le operazioni di controllo, l'aggiornamento sulle varie politiche di licenza, è uno degli impegni più pesanti, visto il numero di clausole e la velocità con cui cambiano.

>> La parola alla difesa!

Enzo Borri parla ovviamente dal punto di vista di chi persegue i reati, ma noi abbiamo voluto sentire anche l'altra campana, quella di chi difende gli imputati. Per questo, abbiamo chiesto al nostro "consulente legale", TuonoBlu, di fare un po' di chiarezza su alcuni aspetti che vengono spesso equivocati.

Hacker Journal: Ma le Forze dell'Ordine possono perquisire la casa (o l'azienda) di chiunque?
TuonoBlu: No. Per poter fare una perquisizione le Forze dell'Ordine devono avere un mandato emesso da un magistrato. Questo passaggio può essere evitato solo in alcuni casi: per esempio, se entrano in un locale pubblico (un negozio, un bar...) e vedono copie di software contraffatto, non hanno bisogno di un mandato per effettuare il controllo e la contestazione del reato. Come dire: se sanno che esiste un reato, possono (e devono) intervenire, ma non possono fare perquisizioni arbitrarie a tappeto andando alla ricerca di software pirata. Un altro caso in cui si può operare senza mandato è quello in cui si cercano reati di tipo tributario. Anche nel caso le Forze dell'Ordine intervengano di propria iniziativa, la perquisizione deve essere convalidata da un magistrato entro 48 ore.

HJ: Che ci dici del personale BSA che, a quanto pare, a volte assiste alle perquisizioni?
TB: È abbastanza evidente che un rappresentante ufficiale della BSA, che nell'eventuale processo sarebbe la parte offesa, sarebbe troppo di parte, e non può quindi avere un ruolo attivo nel procedimento (per esempio, un dipendente BSA non può essere Ausiliario di Polizia Giudiziaria, che deve essere "neutrale").

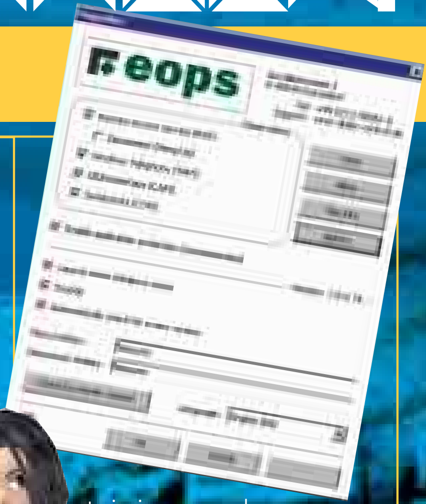
HJ: Riguardo ai sequestri indiscriminati di apparecchiature di vario tipo, com'è la situazione?
TB: A differenza delle intrusioni in sistemi altrui, nel caso della pirateria software il corpo del reato è costituito dai soli dati, ed eventualmente da apprecchi di duplicazione (un masterizzatore per esempio). Le autorità dovrebbero quindi limitarsi a copiare i dati su un CD su cui applicano un sigillo digitale. La Procura di Pescare per esempio agisce in questo modo, ma non tutte sono altrettanto evolute tecnologicamente, anche se le cose stanno migliorando rispetto al passato. In ogni caso, bisognerebbe chiedere che vengano posti sotto sequestro al massimo l'hard disk e un eventuale masterizzatore.

HJ: Ma i reati legati alla pirateria sono ugualmente gravi per le aziende e per i privati, o c'è una distinzione?
TB: Su questo punto non c'è un'interpretazione univoca da parte dei giudici. Qualcuno sostiene che il privato "trae comunque un profitto" dall'utilizzo di software pirata, e condanna l'imputato. Per altri invece, specialmente nei casi di software specializzato e molto costoso, un privato non trae un profitto perché comunque non acquisterebbe mai il pacchetto originale. La mia interpretazione è ovviamente la seconda, ma come dicevo ogni sentenza fa un "caso a sé", e sarebbe auspicabile un chiarimento in materia da parte del Parlamento o del Governo.

COME DIFENDERSI DA PROGRAMMI MALIZIOSI E BOLLETTE SALATE

NIENTE PIÙ DIALER!

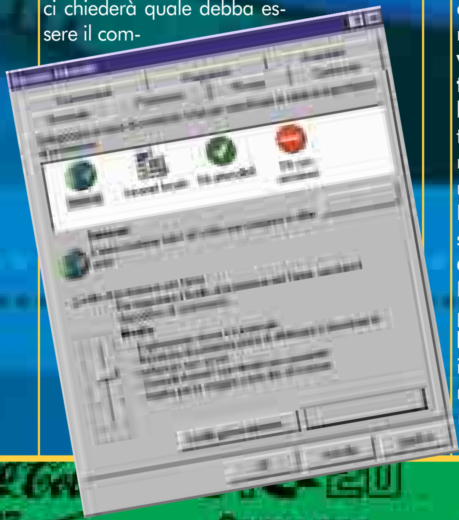
ALTRO CHE GRATIS... SI POSSONO SPENDERE CIFRE ENORMI SENZA NEMMENO ACCORGERSENE



Su tanti siti porno o che distribuiscono loghi e suonerie per cellulari svetta sempre una parola: gratis. Ma se si osserva la bolletta del telefono, si scopre che **certi sfizi si possono pagare molto cari...**
La colpa è dei dialer: dei programmini che staccano la connessione telefonica al provider, e la riattivano su un numero diverso, con tariffe che possono arrivare a quasi due euro al minuto. Se da un lato alcuni siti avvisano chiaramente l'utente di come funziona il meccanismo e su quali sono i costi dell'operazione, **tanti altri cercano di abbindolare i propri visitatori**, mascherando il donwload del dialer, o facendolo avvenire in automatico all'apertura della pagina Web.

>> Schermi alzati!

La prima cosa da fare, è **impostare le protezioni del browser** per impedire l'esecuzione automatica dei programmi scaricati da Internet. In questo modo ogni volta che si scaricherà un dialer, volontariamente o meno, apparirà una finestra di avvertimento che ci chiederà quale debba essere il comportamento da tenere.



Su Internet Explorer, è buona norma **mantenere il livello di protezione per lo meno sul livello Medio** (Alto è meglio, chiede conferma per ogni cookie ricevuto, anche quelli pienamente legittimi...).
Se poi prestate attenzione all'eventuale finestra del download (varia a seconda del browser), potrete bloccare il prelievo del file sul nascere, evitando di scaricare anche centinaia di Kbyte in una sola sessione.
Questo però potrebbe non bastare, specialmente se il computer viene usato da **persone poco esperte (un famigliare o un collega), che possono incappare nella trappola** e far spendere alla famiglia o all'azienda decine (o centinaia!) di euro al mese.

>> Proteggiamoci!

In queste situazioni è utile installare un programma come Dialer Control (**www.dialer-control.de**); si tratta di un software completamente gratuito che si attiva al lancio di Windows e rimane residente in memoria. **Ogni volta che intercetterà le mosse tipiche mosse di un dialer malizioso** (prelievo di un dialer noto, tentativo di disconnessione della linea telefonica, creazione di una nuova impostazione di Accesso Remoto, attivazione della Connessione Guidata Internet), **DC impedirà l'operazione.**
Il bello è che le impostazioni di protezione **possono essere bloccate con una password**, in modo che (anche volendo), nessuno possa utilizzare dialer non autorizzati. Tutte le impostazioni, compresa la password, possono essere applicate facendo doppio clic sull'icona con la D gialla, che si trova nella barra delle applicazioni di Windows, vicino all'orologio.



>> Sfida aperta

Per chi produce e distribuisce i dialer, **un programma come Dialer Control è una spina nel fianco**, e per questo hanno cominciato a modificare i propri programmi per cercare di **aggirare le barriere erette attorno al modem da Dialer Control**. Alla Eops (la casa che produce Dialer Control) non si sono scomposti più di tanto: hanno cominciato a rilasciare versioni aggiornate del programma, in grado di contrastare i dialer di nuova generazione. In più, **le versioni più recenti di Dialer Control hanno una funzionalità di verifica automatica della presenza di nuove versioni**: basta fare clic sul pulsante Check for new versions della finestra principale del programma, per vedere se esistono nuove difese da scaricare.

COME CANCELLARE (DAVVERO!) FILE RISERVATI O "COMPROMETTENTI"

A VOLTE RITORNANO



Anche se avete cancellato un documento e svuotato il cestino, il contenuto può essere facilmente recuperato con poca fatica

Siete sicuri di aver davvero cancellato i dati dal vostro disco, o li avete soltanto "nascosti sotto al tappeto"?

È abbastanza evidente che sui i moderni sistemi operativi con interfaccia grafica, dopo aver spostato un file nel cestino, questo non viene effettivamente cancellato, ma rimane accessibile finché non si effettua lo svuotamento del cestino. Quello che la maggior parte delle persone non sa, è che **il file può essere facilmente recuperato anche dopo che si è svuotato il cestino**, e che quindi qualsiasi utente appena appena esperto e abbastanza motivato può recuperare qualsiasi documento. E appropriarsi delle informazioni in esso contenute.

>> Niente di anormale

Il tutto non suona strano né singolare a chiunque sappia come funziona il file system di un computer. Quando si registra un documento sul disco rigido, i dati vengono registrati come sequenza di zero e uno in una determinata posizione del disco; per sapere dove recuperare quel determinato documento, il sistema deve però tenere un "registro" in cui segna la posizione tutti i file. **Quando si cancella un file** con le normali funzioni del sistema operativo, questo viene "marcato" come cancellato, e vengono eliminati i riferimenti a esso, ma **i dati veri e propri non vengono nemmeno toccati**. Facendo un paragone con il mondo fisico, supponendo di voler gettare via il libro contenuto in una biblioteca il sistema operativo non farebbe altro che eliminare la scheda del libro dall'indice delle opere, e appiccicare un'etichetta con scritto "eliminato" sulla copertina del libro. Il libro rimarrebbe nella sua posizione fino al momento in cui ci sarà bisogno di spazio per inserire un altro libro (cioè registrare un altro file). Solo quando sarà necessario registrare

> **?** **Formattazione** a basso livello Un processo analogo alla semplice formattazione di un disco, ma che prevede anche l'azzeramento di tutti i bit.

NEWBIE

sopra alla stessa porzione di disco, i dati verrebbero eliminati (anche in questo caso è possibile recuperare i dati scritti in precedenza, ma qui arriviamo a soluzioni da fantascienza, che richiedono molto tempo e apparecchiature speciali). Insomma, se non vengono "aggiunti altri libri", basterebbe passare in rassegna gli scaffali per trovare (e leggere!) tutti i dischi erroneamente considerati eliminati. E questo è più o meno quello che fanno i programmi come Norton UnErase o R-Undelete di R-tools Technology.
Se pensate di poter stare tranquilli, perché avete riformattato il disco, vi facciamo subito preoccupare: quando si formatta il disco con le varie "modalità rapide", non si fa nient'altro che gettare via il "registro" dei file (la File Allocation Table); **ancora una volta, i dati rimangono dove sono sempre stati: sul disco.**

>> Situazioni da paura

Qualcuno starà già tremando pensando al fatto che tutte le immagini delle signorine simpatiche e disinibite che ha cancellato dal suo computer possono essere facilmente riportate alla luce da una mamma o una fidanzata un po' smanettone. Questa però è una delle situazioni meno gravi. **Provate a pensare a cosa può accadere dopo aver venduto il computer a uno sconosciuto** o, (come spesso accade), quando il vecchio computer di un dirigente di un'azienda viene passato a un assistente (magari frustrato per il fatto che il boss ha appena avuto il computer nuovo e, come al solito, a lui toccano gli scarti...). **Informazioni e comunicazioni riservate, codici di accesso a banche dati o conti correnti, accordi strategici... tutto nelle mani del primo che passa.**
Ma c'è di peggio: a causa di un baco di certe versioni di Office, vi potreste trovare a inviare documenti che contengono anche porzioni di file cancellati. Quando Word crea un nuovo documento, riserva sul disco un certo spazio, nel quale vengono memorizzate insieme alle informazioni necessarie all'apertura del documento (font, stili, lingua eccetera) anche tutte le versioni precedenti e le informazioni necessarie a recuperare un documento in caso di blocco del computer. Come dicevamo lo spazio viene "riservato" per il documento di Word all'atto della sua creazione: tornando al nostro esempio, Word si "prende per sé" un paio di scaffali della libreria, senza però svuotarli dai libri precedentemente cancellati. Quando si salva il documento, i dati contenuti in quella porzione di hard disk vengono inglobati: aprendo il documento con Word, non si noterà nulla di diverso (perché quei dati non fanno parte del documento), ma **se si apre il file .doc con un editor di puro testo, o con un editor esadecimale, si potranno leggere frammenti di altri documenti.** Se non ci credete, fate una prova, magari utilizzando un disco dal quale sono stati cancellati molti file di testo: c'è da rabbrividire...

> UN FAMIGLIARE O UN COLLEGA IMPICCIONE POTREBBERO CON POCO SFORZO LEGGERE I FILE CHE CREDEVATE DI AVER CANCELLATO DAL VOSTRO COMPUTER

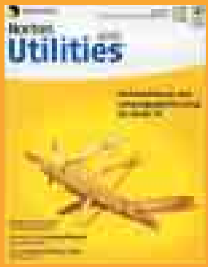
?

NSA National Security Agency. L'agenzia per la sicurezza nazionale americana. Il suo motto è "Offrire e proteggere informazioni vitali attraverso la crittologia".



Secondo qualcuno, questi signori sono i più tosti nel recuperare informazioni di ogni tipo, anche da dischi apparentemente cancellati.

I PROGRAMMI PER RESUSCITARE UN FILE...



NORTON UTILITIES
Nel popolare pacchetto di utility, il programma UnErase permette di recuperare file cancellati, anche avviando da DOS (cosa consigliabile).

DISK INVESTIGATOR
Un programma che legge i dati grezzi direttamente dall'hard disk, bypassando le informazioni fornite dal sistema. È gratuito e si scarica da www.theabsolute.net/sware/dskinv.html

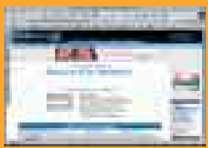
...E QUELLI PER ELIMINARLO DAVVERO

PGP DISK
La funzionalità Document Wipe di PGP Disk consente di sovrascrivere file con dati casuali in più passaggi, a scelta dell'utente.



ACTIVE@ KILL DISK - HARD DRIVE ERASER
Un software gratuito ma che, nella sua versione a pagamento è conforme alle direttive per la "pulizia e disinfezione dei dati" del Dipartimento della Difesa americano. Si scarica da www.killdisk.com/eraser.htm

VARI FREEWARE
All'indirizzo www.webattack.com/freeware/security/fwerase.shtml sono elencati svariati programmi gratuiti per la cancellazione sicura dei file.



COME CANCELLARE (DAVVERO!) FILE RISERVATI O "COMPROMETTENTI"

CON I MICROSCOPI A FORZA MAGNETICA SI POSSONO LEGGERE ANCHE I DATI CANCELLATI E SOVRASCRITTI

>> Come fare piazza pulita

Per essere sicuri di aver davvero cancellato un documento, bisogna quindi utilizzare un programma che scriva **una diversa sequenza di dati binari casuali** nella stessa porzione di disco in cui si trova il file da eliminare. Esistono svariati software di questo tipo, e la funzione di "cancellazione sicura" viene inclusa anche in parecchie suite di utility (come le famose Norton di Symantec) o in programmi di privacy e crittografia (tipo Pgp). Alcuni programmi si limitano a cancellare in modo sicuro un documento ancora perfettamente visibile: si seleziona il file desiderato, e questo verrà cancellato in modo sicuro e irrevocabile (occhio, prima di cancellare documenti che vi potrebbero ancora servire...). **Altri programmi invece lavorano sui file che sono già stati cancellati, facendo un'operazione di "ripulitura"** di tutte quelle aree del disco che sono state marcate come "area libera" per la scrittura di nuovi file, ma che –come abbiamo visto– potrebbero contenere dati. Entrambe le funzionalità sono utili, e la maggior parte dei programmi di "cancellazione sicura" sono in grado di svolgerle entrambe.

Prima dicevamo che i programmi di cancellazione sicura non si limitano a porre a zero (o uno) i bit dell'area occupata dal file, ma scrivono sul disco una "diversa sequenza di dati binari casuali". Questa differenza può essere considerata una sottigliezza irrilevante per la maggior parte degli utenti (che vogliono proteggere la propria privacy da colleghi o famigliari curiosi), ma per qualcuno assume un'importanza... vitale.

>> La paranoia non è mai troppa

Anche se sovrascritti e non più rilevabili dalle testine dell'hard disk, i dati cancellati lasciano sulla superficie del disco **una "traccia" magnetica molto debole, ma identificabile con strumenti adeguati**, come un apparecchio per la Microscopia a Forza Magnetica (MFM). Con lo strumento giusto (alcuni modelli di microscopi MFM sono già equipaggiati per analizzare superfici di hard disk...), **una persona preparata potrebbe "vedere" i bit cancellati con la stessa facilità con cui un testo a matita cancellato con una gomma può essere letto tenendo il foglio di carta in controluce.**



Questa immagine è stata ricreata artificialmente per dimostrare come essa potrebbe rivelare un documento di Word che abbia incluso frammenti di informazioni casuali presi dalla memoria e dal disco. I programmi che soffrono di questo problema sono Microsoft Word 6.0 e 7.0, e la versione 7.0 di PowerPoint ed Excel. Microsoft ha rilasciato aggiornamenti che lo correggono.

Scrivendo una sequenza di soli "zeri" o "uno", sul disco, le informazioni possono essere ancora recuperate in base alla differenza di forza magnetica che esiste tra i bit che prima della cancellazione contenevano uno zero, e quelli che prima contenevano un uno. Tornando al nostro foglio col testo cancellato, è un po' come applicarci sopra un foglio di carta velina: in controluce il testo si nota comunque. Proprio per questo, i programmi "seri" sovrascrivono i dati con **una sequenza casuale di dati, e non si limitano a una sola riscrittura, ma eseguono svariati passaggi** (in alcuni casi, il numero è a discrezione dell'utente).In genere, **tre passaggi sono considerati un ragionevole compromesso tra sicurezza e praticità**: il tempo di cancellazione infatti aumenta in modo proporzionale al numero di passaggi.

Qualcuno obietta che il recupero di informazioni da porzioni di disco sovrascritte con altri dati **è roba che si vede solo nei film di spionaggio**. Sarà, ma l'NSA sembra prendere sul serio la questione, e il Dipartimento della Difesa americano ha realizzato una direttiva per l'eliminazione sicura dei dati. **Se si preoccupano loro, perché non dovremmo farlo anche noi?**



La superficie magnetica di un disco Zip analizzata con un microscopio a forza magnetica.

PER SAPERNE DI PIÙ...

www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html
Una vera bibbia sugli aspetti più scientifici della lettura di informazioni dai supporti magnetici

ftp://ftp.cerias.purdue.edu/pub/lists/best-of-security/326
Brevetto dell'NSA per il rilevamento dei campi magnetici in supporti sovrascritti.

www.all.net/books/standards/remnants
Guida alla comprensione dei dati residui nei sistemi informatici del Computer Security Center.

Uplink
il simulatore di hacking



Avete già finito Try2hack ma vi è rimasta la voglia di cimentarvi in sfide sempre più impegnative? Provata allora ad hackerare i mainframe di grosse compagnie..., ma per gioco!

QUANDO L'HACKING DIVENTA VIDEOGIOCO

Dopo questa doverosa introduzione passiamo alla descrizione di questo rivoluzionario simulatore della Introversion. I creatori di questo titolo sono da premiare per la loro originalità e per avere avuto il coraggio di andare controtendenza (che è poi la filosofia che sta dietro al gioco in questione). E si, perchè gli sviluppatori, un gruppo di giovani studenti di ingegneria di Londra, hanno **tralasciato l'aspetto grafico a favore di una buona programmazione** (ormai siamo abituati sempre più a prodotti graficamente superlativi ma pieni di bug).



Ma di cosa si tratta? Il titolo in questione va sotto la categoria di" simulatore". **Dovrete calarvi nei panni di un giovane hacker agli inizi della sua attività**, ingaggiato da una associazione, la Uplink. Il gioco è ambientato in un ipotetico 2010, e **l'interfaccia grafica ricrea appunto un gateway, caratterizzato da apparecchiature sofisticate e componenti hardware da far rabbrividire**. Le musiche ricreano perfettamente l'atmosferà e in certi istanti diventerà incalzante, facendo aumentare l'adrenalina al massimo!

>> Da newbie a guru

Ovviamente, comincerete con un semplice computer e un modem, ma superando le varie missioni che via via vi saranno proposte, **verrete ricompensati con del denaro che vi servirà ad accrescere le potenzialità del computer** e fare così lavoretti sempre più sofisticati... Tra le componenti hardware da installare ricordiamo modem, cpu,memoria ram, sistemi di monitoraggio e altro ancora. Ma non è finita qui: potete (anzi dovete, se volete avanzare di livello) **acquistare anche software e qui si va dai rilevatori di password a sofisticati programmi di crittografia**.
Pur essendo un gioco interamente offline, la nuova patch rilasciata dagli sviluppatori aggiunge tra il software da acquistare anche un client irc per poter chattare all'interno del gioco. E, magari, potere sfidare in tempo reale un'altro hacker vero e proprio... Con queste premesse capirete che "il gioco si fa duro"!

>> Come inizio a giocare?

Prima di accedere al gioco dovrete registrarvi come agente, inserendo un vostro nick ed una password. Dopodiché, dovrete scegliere la postazione del vostro gateway e il gioco è fatto. Vi troverete di fronte ad un desktop e riceverete subito una e-mail che vi presenterà quello che sarà il vostro nuovo lavoro. Ma prima di"lavorare" la Uplink vuole mettervi alla prova. In una successiva mail, infatti **vi inviterà ad entrare da remoto in un sistema protetto da password e rubare un file specifico**. Una volta fatto ciò, salvate il file nella vostra memoria e mandate una mail alla compagnia che vi ha ingaggiato, con allegato il file in questione....Et voilà,da questo momento avrete accesso ad una sfilza di missioni, ovviamente secondo il vostro grado di preparazione le missioni che vi offriranno saranno sempre più difficili, e ovviamente meglio ricompensate;-).

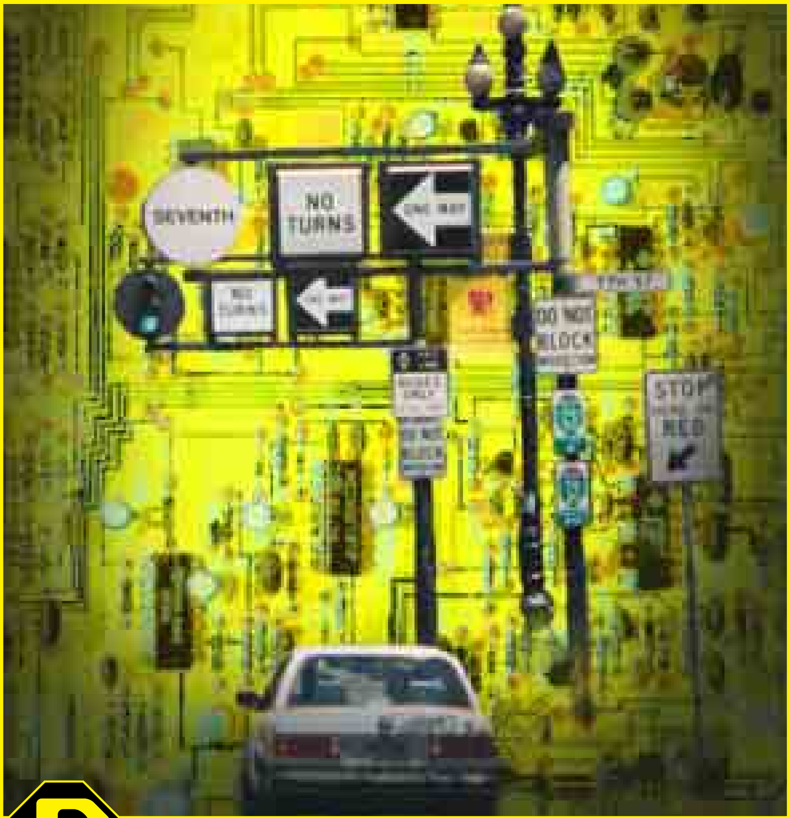
Antonino Benfante

Uplink esiste per Windows e Linux, e costa 33,99 Euro. Dal sito del produttore, all'indirizzo www.introversion.co.uk, si può scaricare una versione demo.

ISTRUZIONI E TRUCCHI PER ASPIRANTI OPERATORI

IRC CREA E GESTISCI IL TUO CANALE

Gestire un canale significa avere un grande potere su tutti gli altri utenti, ma (come in teoria dovrebbe accadere anche nel mondo reale), il potere significa anche responsabilità



Dopo la prima infarinatura del numero scorso su cosa sia Irc, la sua struttura e i primi passi da muovere per entrare in questo mondo, spingiamoci ora più in profondità nell'argomento, cercando di analizzare come si può aprire e gestire un canale.
Partiamo dal presupposto che su Irc esiste circa tutto, e quindi si possono trovare canali su ogni materia dello scibile umano. Se però avete l'esigenza di avere un vostro canale personale (o volete semplicemente togliervi lo sfizio), in queste pagine vedremo tutte le procedure necessarie, i privilegi e i possibili problemi che potrete incontrare.
Un qualunque utente può aprire un nu-

>> Tutti OPeratori

mero illimitato di canali semplicemente eseguendo il comando in linea

```
/join #ilmioprimocanale
```

Supponendo che questo canale non esista già in precedenza si avrà una schermata con il vostro unico nome in alto a destra preceduto dalla @. **Quel simbolo vi attribuisce lo status di operatore del canale** con tutti i privilegi ed i doveri che l'accompagnano.
La parte più delicata riguardante la gestione di un canale è il decidere chi e cosa è ammesso, il tipo di argomento trattato (libero oppure limitato ad un soggetto specifico), gli utenti autorizzati ad accedervi e quant'altro comunque rientri nella gestione.
Le modalità di canale sono per così dire le regole che voi potete impostare e che necessariamente devono essere seguite. In generale la sintassi è data dal comando

```
/mode #canale +/-lettera parametro
```

dove + indica l'attuazione e – la soppressione del modo specificato.

>> Modalità di un canale

Ora vediamo nel dettaglio le modalità di canale, suddividendole in quelle applicabili al canale ed in quelle applicabili agli utenti.

Modalità i (invite only): definisce la modalità invito per il canale. Solo gli utenti che siano stati "invitati" possono accedervi, agli altri sarà negato il permesso con un output del tipo "Can't access the channel, invite only". Si imposta col comando `/mode #canale +i`. Gli utenti possono essere invitati sul chan solo da un utente all'interno del chan stesso con il comando `/invite`

```
nick #canale
```

Modalità l (limit): definisce il numero massimo di utenti all'interno del canale. Chi tenta di entrare dopo che la soglia è stata raggiunta riceve un output del tipo "chan is full". La sua sintassi è `/mode #chan +l xx`, dove xx è il numero arbitrario di soglia.

Modalità n (no external messages): fa sì che gli utenti non presenti all'interno del canale non possano inviare messaggi in pubblica.

Modalità k (key): definisce la password di accesso al canale stesso. Si imposta col comando `/mode #canale +k xxxxxx` dove xxxxxx è ovviamente la password desiderata. Un utente che cerchi di entrare in un canale +k riceverà un output del tipo "need correct key". Per entrare in un chan +k il comando da utilizzare è `/join #chan xxxxx`

Modalità s (secret): impostazione di canale che permette di non dare info sul canale stesso, non apparire col comando `/list` e neppure nel `/whois` di un utente a meno che entrambi siano all'interno di quel chan.

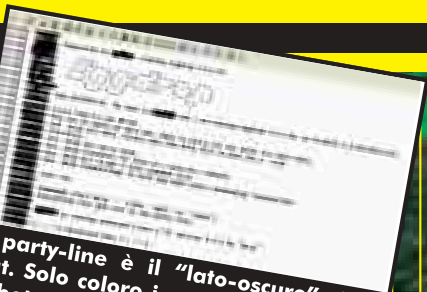
Modalità t (topic): se impostata non permette agli utenti –o di cambiare il topic del canale.

Modalità m (moderated): il canale in questa modalità si definisce "moderato", ovvero solamente i +o oppure gli utenti con modalità +v possono interagire in pubblica, mentre a tutti gli altri è interdetta. Restano ovviamente attive per chiunque le query personali.

Modalità p (privato): modalità obsoleta e non più utilizzata che non permette la visione del nome del canale con un /list, ma fornisce altre info richieste.



nell'esempio vedete il ban settato per l'utente sdsds sul chan #sdsds...che fantasia ho avuto! Nella copia del /whois potete vedere la mask ed i dati necessari per settare il ban



la party-line è il "lato-oscuro" della chat. Solo coloro i quali sono "addati" sui bot ed i loro owner vi possono accedere. In questa chat parallela si configurano i settaggi dei bot e si istruiscono sui comportamenti da tenere.

>> Modalità degli utenti

Modalità o (operatore): assegna i privilegi di operatore al nick selezionato. Gli operatori hanno "superpoteri" sia sugli utenti normali che sugli altri operatori del canale. Si imposta con `/mode #chan +o nick`.

Modalità v (voice): l'utente che usufruisce di questo beneficio è autorizzato a parlare nei canali +m. È spesso inutile, perché i canali sono normalmente impostati come –m, ma viene lo stesso attribuito ad alcuni utenti come segno di simpatia nei loro confronti.

Modalità b (ban): consente di impostare un divieto di ingresso a qualunque utente abbia una mask uguale al ban settato. L'identità di chiunque su Irc è data nel seguente formato: nick!username@host.name, dove nick è il nick utilizzato, username è il nome utente, host.name è l'indirizzo IP da cui ci si connette.
Nell'impostazione dei ban esistono dei caratteri speciali che possono essere utilizzati; questi sono (*) e (!). Il primo identifica un qualunque gruppo di caratteri compreso nessuno, mentre il secondo indica un qualunque carattere singolo ma non nessuno. Ovviamente questi divieti possono essere più o meno specifici. Se per esempio abbiamo a che fare con un utente indesiderato che si collega con un IP fisso, settare un ban sarà molto semplice e non correremo il rischio di includere nel divieto anche qualche altro utente incolpevole. Considerando per assurdo che l'utente Ciao abbia un IP statico 111.222.121.212, settando il ban

```
/mode #chan +b ciao!ciao-mask@111.222.121.212
```

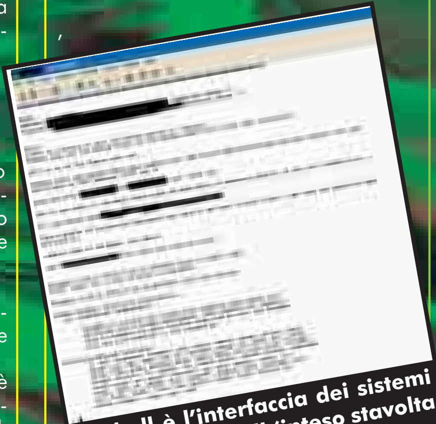
siamo certi che quell'utente non possa entrare di nuovo nel canale. Potrebbe però cambiare mask, da qua la necessità di allargare il ban che potrebbe prendere la forma di

```
/mode #chan +b
*!*@111.222.121.212
```

Nel caso di un utente con dialup ed IP dinamico la questione è più complessa considerato il fatto che normalmente una volta sconnesso e riconnesso l'IP cambia. Se per assurdo Ciao avesse come mask

```
ciao!ciaomask@ppp-151.27.10.10.libero.it
```

,



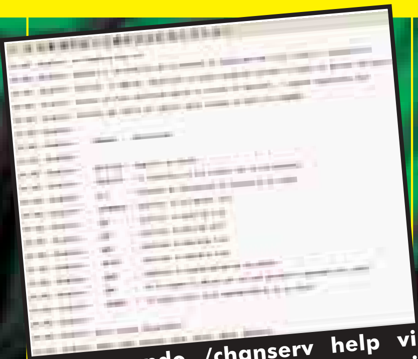
la shell è l'interfaccia dei sistemi unix-like. Su shell (inteso stavolta come account su un server remoto) giacciono i bot.

possiamo provare a settare un ban del tipo

```
*!*ciaomask@ppp-*.libero.it
```

con la speranza che usi sempre lo stesso provider per collegarsi. Teniamo comunque presente che in questo modo non settiamo un ban specifico, quindi se esiste un altro utente che usa libero.it ed ha come parte della mask "ciaomask" questo si troverebbe bannato dal vostro canale pur non sapendo il perché. Il consiglio è quindi quello di settare ban sempre il più specifici possibile evitando così di tagliare fuori troppi utenti. Ovvio che se settiamo un ban

ISTRUZIONI E TRUCCHI PER ASPIRANTI OPERATORI

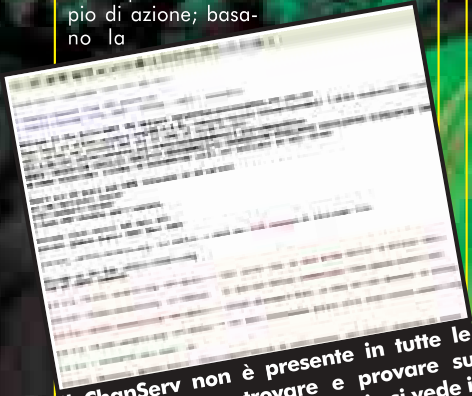


col comando /chanserv help vi viene proposto un help online coi comandi principali, le loro azioni e, a richiesta, le stringhe di uso.

!@*.jp mai nessuno che si connette con un server giapponese potrà entrare all'interno del nostro chan, sia che siano "buoni" sia che siano "cattivi"

>> La sicurezza del canale

Se possedete un canale, prima o poi **comincerete a pensare che qualcun'altro prima o poi cercherà di rubarvelo.** Ci sono varie modalità per attuare queste azioni, ma le più utilizzate sono certamente i flood, i cloni, i collide. **Per flood si intende l'invio di un'enorme quantità di dati** a un client o ad un canale, azione che spesso porta alla sconnessione del client attaccato e quindi all'eliminazione delle persone all'interno del chan. I cloni hanno lo stesso princi pio di azione; basano la



il ChanServ non è presente in tutte le reti. Lo potrete trovare e provare su azzurra.net. In questo esempio si vede il riconoscimento di un nick registrato da parte dell'utente inserendo la password.

loro forza sulla loro "replicazione" con più client aventi lo stesso IP, ed agiscono con un attacco tipo mircforce di flood. **I collide sono tecniche più complesse ma allo stesso tempo più efficaci.** In soldoni si basano sul fatto che su Irc non ci posso essere due utenti con lo stesso nickname. In caso si realizzi questa situazione, entrambi i client vengono sconnessi dal server. I metodi di realizzazione di tali strategie e la loro attuazione pratica saranno comunque trattati in maniera più approfondita nell'ultimo di questa serie di articoli.

>> Registrare un canale

Su IRCnet non è prevista la registrazione di nickname o di canali, ma su altre reti come **azzurra.net** c'è un servizio, il `chanserv`, che è preposto a questo scopo. Potete facilmente scoprire se è presente e come si usa ChanServ semplicemente digitando

```
/chanserv help
```

oppure

```
/msg chanserv help
```

Vi apparirà una lista di comandi e su ognuno di essi potrete richiedere aiuto specifico.

>> BOT: il portiere di notte

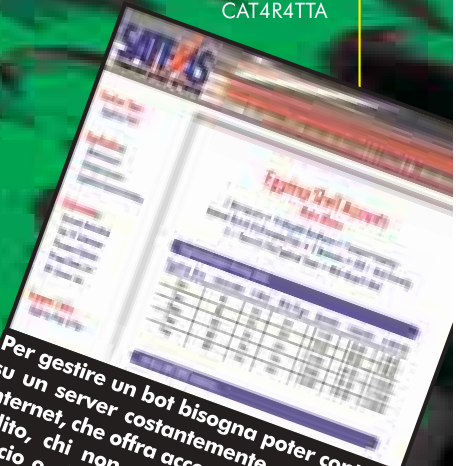
Cosa succede quando è tardi e si deve andare a dormire? Beh...se siete gli ultimi ad uscire da quel chan allora il canale "andrà a dormire" con voi. Nel momento in cui un canale resta vuoto cessa di esistere, e con esso tutte le impostazioni /mode effettuate con tanto sudore della fronte. Per ovviare a questo problema si usano i Bot. **Si tratta di particolari client che giacciono su shell remote perennemente connesse alla rete e totalmente gestibili e programmabili in remoto.** Hanno status di operatore del canale e sono completamente asserviti ai vostri ordini, fanno tutto ciò che voi gli dite di fare e...non sporcano :D

Ma come tutto al mondo anche i Bot non sono solo rose e fiori. Innanzitutto hanno un costo; beh...mica avrete pensato che qualcuno vi permettesse di tenere dei client sui propri server, con tutto ciò che ne consegue tipo attacchi dDoS, gestione e spese, senza farvi pagare un euro?!?!

Oltre al costo, l'altra rottura è la configurazione; nulla di particolarmente complesso, ma pur sempre cose da studiare e su cui impratichirsi perché all'inizio niente è molto intuitivo. Considerando inoltre il fatto che **normalmente giacciono su piattaforme linux/freeBSD e vanno gestiti da shell con cui l'utente medio non ha confidenza, le cose si complicano un po'** per chi arriva da Windows e ha poca esperienza. I Bot, come vedremo dettagliatamente sul prossimo numero, di certo vi daranno una mano a gestire i vostri canali, vi daranno una posizione di vantaggio rispetto a tutti gli altri utenti, ma sono pur sempre delle macchine "stupide" che se non sono istruite a dovere possono creare problemi.

Nell'articolo che troverete sul prossimo numero entreremo più in dettaglio sulla programmazione dei Bot, e parleremo delle IRCwar, guerre a colpi di bit che si combattono sui canali Irc. Buon divertimento sui vostri nuovi canali e mi raccomando: non dimenticatevi di dirmi quali sono!!!!!

CAT4R4TTA



Per gestire un bot bisogna poter contare su un server costantemente collegato a Internet, che offra accesso a una shell. Di solito, chi non può impostarne uno in ufficio o all'università, deve rivolgersi a servizi a pagamento, con costi che partono da circa 10 dollari al mese.

IDENTIFICATION ORDER NO. 9
September 26, 2002

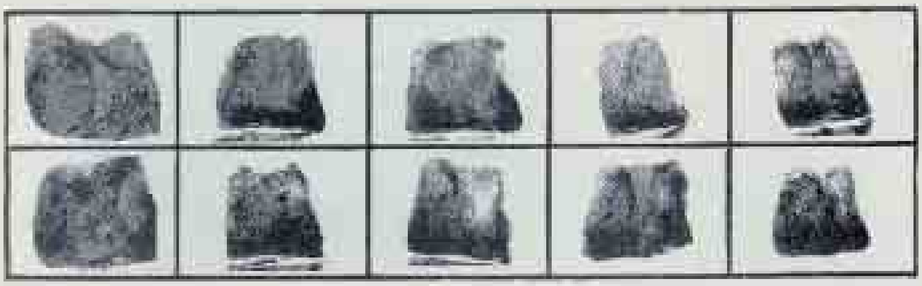
DIVISION OF INVESTIGATION
H.J. DEPARTMENT OF NET
CERNUSCO S.N., MI

Fingerprint Classification

16 0 5 U 001 20
1 17 U 001

WANTED

NAME: SubSeven
TYPE: Cavallo di Troia
ALIAS: Backdoor-G, Backdoor.SubSeven, Sub7
DATE OF BIRTH: May 1999
AUTOR: Mobman





Azioni compiute:

A seconda delle versioni, SubSeven può effettuare circa un centinaio di diverse azioni, tra queste, le più pericolose sono:
- Registra suoni dal microfono del computer attaccato;
- Cattura immagini da una eventuale Webcam;
- Legge le password dal disco e dalla memoria;
- Registra i tasti premuti dall'utente, anche quando è offline, e li invia all'attaccante.



- Notifica all'attaccante la presenza online della vittima;
- Cattura l'immagine dello schermo;
- Apre un server Ftp che permette all'attaccante di scaricare o cancellare qualsiasi file della vittima;
- Modifica il registro di Windows.
- Esegue applicazioni.
- Inserisce comandi manuali.
- Permette all'attaccante di scrivere in qualsiasi applicazione aperta.

Mezzi di contagio:

- Apertura di file eseguibili infetti ricevuti via email, attraverso una chat Dcc in Irc, o scaricati da siti non affidabili (tipicamente, siti "warez", "crackz" o porno);
- Installazione diretta da parte di un attaccante che abbia accesso fisico alla macchina che vuole controllare (a casa, in ufficio, in un negozio...).

Tecniche utilizzate:

Il programma server si installa nella direcory Windows con il nome del programma che ha veicolato l'infezione, o usando altri nomi. Dopodiché modifica il registro di Windows associando il programma server a tutti i file con estensione .exe. In questo modo, si assicura di rimanere sempre in esecuzione (ogni volta che si lancia un programma, SubSeven viene attivato). Se il server viene rimosso, nessun programma potrà essere avviato (alcune versioni non danno questo problema).

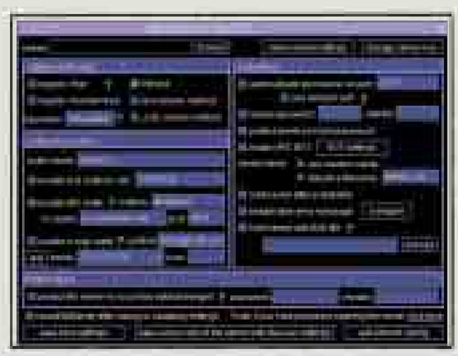
Quando è in esecuzione, è completamente invisibile nella lista dei task, e se trova una connessione Internet aperta, rimane in attesa di comandi da parte del client remoto.

Segni particolari:

SubSeven può essere individuato in questo modo:
- Inserisce nuovi valori nelle chiavi di registro:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
- Inserisce una nuova linea nella sezione [windows] del file win.ini
[windows]
load=
run=c:\windows\sever name.exe
Inserisce una nuova linea nella sezione [boot] di system.ini
[boot]
...
shell=Explorer.exe c:\windows\server name
- Attiva alcune porte TCP, solitamente la 27374, ma la porta può essere cambiata dall'attaccante.

Istruzioni per l'arresto:

Anche un buon antivirus, perfettamente aggiornato, a volte non è in grado di contrastare un cavallo di Troia; l'attaccante potrebbe infatti alterare la funzionalità dell'antivirus, lasciando all'utente una falsa sensazione di sicurezza.



Il modo più sicuro per contrastarlo è quello di consultare il sito www.hackfix.org/ subseven/ per determinare il numero di versione del server e individuare il programma più adeguato per la sua rimozione.

Ulteriori informazioni:

www.europe.f-secure.com/v-descs/subseven.shtml
www.symantec.com/avcenter/venc/data/backdoor.subseven.html

FARSI IN CASA UNO STRUMENTO PER ANALIZZARE LE PORTE APERTE SU UN HOST



Un portscanner in Visual Basic

Come programmarsi con poche stringhe di codice Visual Basic un tool molto utile

In rete se ne trovano tanti, di tutti i tipi e per tutti gli OS. I portscanner sono programmi molto utili in quanto ci **possono servire per constatare quali porte sono "aperte" ovvero in listening su un determinato host** oppure può essere usato in locale per controllare quali porte sono aperte sulla nostra stessa macchina. Ciò ci permette di ricavare varie informazioni da un host come, l'OS su cui gira, i vari tipi di servizi (TCP/UDP) in esecuzione sul sistema eccetera. Vedremo quindi come crearcene uno nostro usando Visual Basic; qui metteremo solo l'occorrente che serve, poi sarete voi ad ampliarlo con altri controlli,comandi,funzioni eccetera. È quindi richiesta una conoscenza base di Visual Basic.

Nella tabella qui a destra potete vedere qquali sono gli oggetti e i controlli di cui avremo bisogno nel nostro progetto.

Per includere il controllo Winsock nel progetto premere control-T nella finestra principale del VB, oppure dal menù Progetto--Componenti…, apparirà un'altra finestrina qui cercare il componente Microsoft Winsock Control (n. versione).

Oggetto	Proprietà	Impostazione
Form	Name Caption	Form1 Portscanner
Command	Name Caption &	cmdScan Scanna!
Command	Name Caption	cmdFerma &Ferma
Command	Name Caption	cmdEsci &Esci
Label	Name Caption	lblHost Host:
Label	Name Caption	lblMsg Porta Iniziale:
Label	Name Caption	lblFinal Porta Finale:
List Box	Name	List1
Text Box	Name	txtHost
Text Box	Name Text	txtPorta 1
Text Box	Name Text	txtFinale 65536
Winsock Control	Name	Winsock1
Temporizzatore	Name Interval Enabled	Timer1 1500 False

>> Iniziamo a Codare...

Passiamo subito ad analizzare il codice...

```
Private Sub cmdscan_Click()
cmdscan.Enabled = False    'Disattivo il
tasto "Scanna!"
cmdferma.Enabled = True    'Attivo il tasto
"Ferma"
List1.clear                  'Pulisco la
list box
Winsock1.Connect txthost.text ,
txtporta.text
'Faccio connettere il Winsock all'host (im-
messo nella text box "txthost",
'e alla porta contenuta nella text box
"txtporta")
Timer1.Enabled = True 'Attivo il temporiz-
zatore
End Sub
```

Commentiamo ciò che abbiamo appena fatto (anche se alcuni commenti ci sono già...). Nella prima procedura, ovvero quando cliccate sul tasto "Scanna!", questo tasto si disattiva mentre si attiverà il tasto "Ferma". Questo perché se per errore cliccate diverse volte sul tasto "Scanna!", il programma vi risponderà kiudendosi con un bel errore di Run Time :).
Poi faccio connettere il winsock all'host immesso nel textbox chiamato <<txthost>> e alla porta che verrà immessa nel text box <<txtporta>> e infine verrà attivato il temporizzatore...

```
Private Sub cmdferma_Click()
Winsock1.Close 'Chiudo il winsock
lblmsg.Caption = "Porta Iniziale:"
'Resetto dinuovo la proprietà caption al
label <<lblmsg>> (vedrete poi xkè...)
Timer1.Enabled = False 'Disattivo il tempo-
rizzatore
```



Ecco per esempio come possono essere posizionati gli oggetti

Controllo degli errori

Ricordatevi che nel codice potete inserire anche delle procedure per la gestione di errori, per esempio "on Error Resume Next", che in caso di errore ripete la procedura senza bloccare l'applicazione, oppure meglio ancora se fate in questo modo:

```
Private Sub cmdscan_Click()
Dim Errore as string 'Dichiaro una variabile stringa
Errore= "Errore durante la scansione" 'Che sarà poi il msg
di errore
On error goto Errore 'In caso di errore vai ad Errore (la
variabile)
...
procedure sub 'Procedure della sub
...
Exit Sub 'Usciamo dalla Sub in caso non mettete Exit Sub
anche
          'se l'errore non esiste il msg sotto verebbe lo
stesso visualizzato

Errore:
 msgbox Errore,vbokonly + vbcritical,"Scanner" 'Il msg che
verrà visualizzato in caso di errore
End Sub
```

(NB.: In VB c'è l'enunciato Err.(opzione) che gestisce gli errori, quindi anche un Err.Description sarebbe un alternativa della procedura sopra descritta)

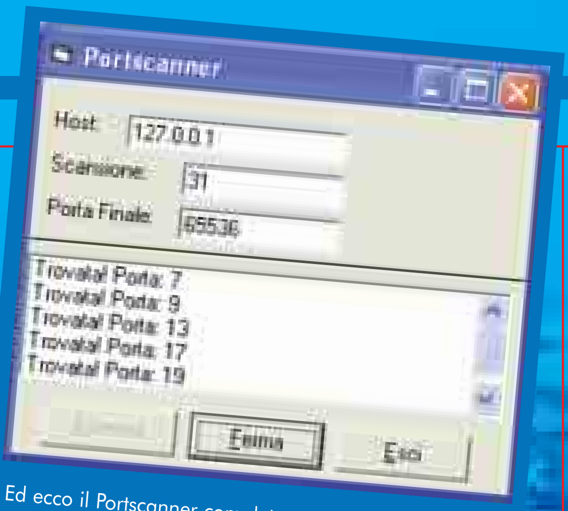
```
cmdferma.Enabled = False 'Disattivo il ta-
sto "Ferma"
cmdscan.Enabled = True    'Riattivo il ta-
sto "Scanna!"
End Sub
```

Cliccando sul tasto Ferma, la scansione verrà bloccata, disattivo il tasto "Ferma" (per lo stesso motivo del tasto "Scanna!" nel primo spezzone di codice...), riattivo il tasto "Scanna!". Naturalmente quando riavvio la scansione il winsock si riconnetterà alla porta che sta nel <<txtporta>> e una volta riavviata la scansione la lista si pulisce...

```
Private Sub cmdesci_Click()
if msgbox("Chiudere il programma?",vbYesNo
+ VbInformation, "Scanner")=vbNo then
form1.visible = true
else
Unload Me
End If
End Sub
```

Prima condizione del codice ovvero, quando cliccheremo sul tasto "Esci" ci comparirà un message box che ci avvertirà di chiudere o meno il programma, se la risposta sarà No allora il programma continuerà ad essere visibile, se invece la risposta sarà Si il programma si chiuderà (semplice no?)uhm...no? SE nel msgbox schiacciate "No" ALLORA mantieni visibile il form ALTRIMENTI chiudilo

```
Private Sub Winsock1_Connect()
List1.AddItem "Trovata! Porta: " & win-
sock1.RemotePort
'Se una porta viene trovata, aggiungo alla
list1 la frase
'e il numero della porta in ascolto sul
server che stiamo scannando
```



Ed ecco il Portscanner completato all'opera in locale :)

```
Call
Timer1_timer 'Chiamo la procedura
Timer1_Timer
End Sub
```

Penso che i commenti abbiano gia spiegato tutto. Praticamente, ogni volta che una porta viene trovata si aggiunge alla list1 la frase "Trovata! Porta:" e affianco il numero della porta, poi chiamo la procedura Timer1_Timer che ci permette di continuare la scansione su altre porta.

>> Il motore dello scanner :)

Passiamo alla parte sostanziosa della faccenda.

```
Private Sub Timer1_Timer()
lblmsg.Caption = "Scansione:" 'Cambio la
proprietà Caption al <<lblmsg>>
txtporta.text = txtporta.text + 1
if Val(txtporta.text) < Val
(txtfinale.text) then  '#1
winsock1.Close '#1
Winsock1. Connect txthost.text ,
txtporta.text '#1
else
MsgBox ("Scanning Completato"), vbinforma-
tion , "Scanner"
Timer1.enabled = false
Call cmdferma_click
End If
End Sub
```

[#1] Condizione
Ogni secondo (visto che l'intervallo del timer è impostato a 1500) il valore del textbox <<txtporta>> sarà incrementato di 1 cifra quindi se per esempio impostiamo come porta un valore iniziale di 1 ad ogni secondo la porta si incrementerà di una cifra ovvero 1,2,3,4... ecc

#1 Se il valore della textbox <<txtporta>> è minore del valore della textbox <<txtfinale>> allora chiudi il winsock per poi ricconnettersi all'host alla porta corrente (di txtporta) oppure se il valore di txtporta corrisponde al valore di txtfinale allora fai apparire il msgbox, ferma il timer e richiama la Sub cmdferma_Click per stoppare tutto :)

Il sorgente del portscanner

```
Private Sub cmdEsci_Click()
If MsgBox("Chiudere il programma?", vbYesNo +
vbInformation, "Scanner") = vbNo Then
Form1.Visible = True
Else
Unload Me
End If
End Sub

Private Sub cmdFerma_Click()
Winsock1.Close 'Chiudo il winsock
lblMsg.Caption = "Porta Iniziale:"
'Resetto dinuovo la propriet‡ caption al label
<<lblmsg>> (vedrete poi xkË...)
Timer1.Enabled = False 'Disattivo il temporizzatore
cmdFerma.Enabled = False 'Disattivo il tasto "Ferma"
cmdScan.Enabled = True   'Riattivo il tasto "Scanna!"
End Sub

Private Sub cmdscan_Click()
cmdScan.Enabled = False   'Disattivo il tasto "Scanna!"
cmdFerma.Enabled = True   'Attivo il tasto "Ferma"
List1.Clear               'Pulisco la list box
Winsock1.Connect txtHost.Text, txtporta.Text
'Faccio connettere il Winsock all'host (immesso nella
text box "txthost",
'e alla porta contenuta nella text box "txtporta")
Timer1.Enabled = True
'Attivo il temporizzatore
End Sub

Private Sub Timer1_Timer()
lblMsg.Caption = "Scansione:" 'Cambio la propriet‡
Caption al <<lblmsg>>
txtporta.Text = txtporta.Text + 1
If Val(txtporta.Text) < Val(TxtFinale.Text) Then  '#1
Winsock1.Close '#1
Winsock1.Connect txtHost.Text, txtporta.Text  '#1
Else
MsgBox ("Scanning Completato"), vbInformation, "Scanner"
Timer1.Enabled = False
Call cmdFerma_Click
End If
End Sub

Private Sub Winsock1_Connect()
List1.AddItem "Trovata! Porta: " & Winsock1.RemotePort
'Se una porta viene trovata, aggiungo alla list1 la
frase
'e il numero della porta in ascolto sul server che
stiamo scannando
Call Timer1_Timer 'Chiamo la procedura Timer1_Timer
End Sub
```

Ciò vuol dire che se noi inseriamo un valore iniziale 1 e uno finale 10 lo scan funge in questo modo

Valore= 1 : connetti, se attiva allora metti nella lista la porta, chiudi winsock... il valore della txtporta cambia dopo 1 sec.
Valore= 2 : riconnetti, se attiva allora metti nella lista la porta, richiudi winsock eccetera.

Questa procedura finirà solo quando il valore di txtporta sarà uguale al valore di Txtfinale

Omega - www.mofcrew.italy.com

NESSUS È UN OTTIMO TOOL GRATUITO PER TESTARE LA SICUREZZA DEI PROPRI SISTEMI DAL PUNTO DI VISTA DEGLI HACKER.

DIFENDIAMOCI... ATTACCANDOCI!

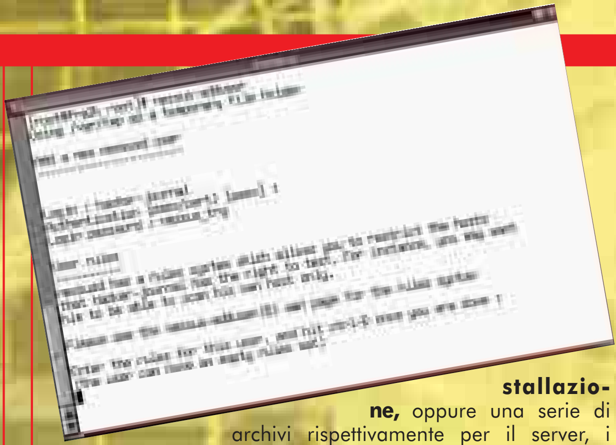
Spesso capita di chiedersi quanto sia al sicuro un sistema, quali porte siano aperte, quali programmi offrano backdoor o possibili DoS.

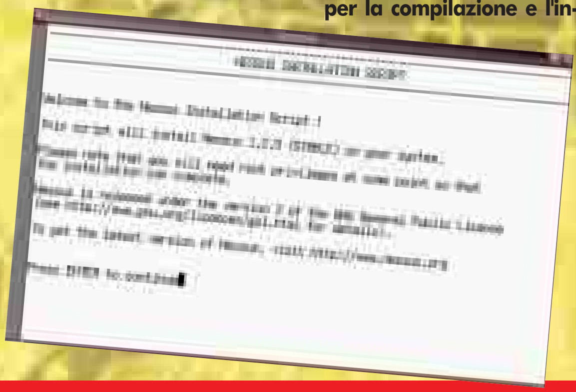
Nessus (www.nessus.org) è un security scanner completamente gratuito e costantemente aggiornato. La sua funzione è quella di analizzare sistemi o intere reti per **individuare quali possono essere le strade che eventuali cracker possono utilizzare per irrompere e fare danni**. Il sistema di plug-in su cui si basa permette di aggiungere con grande facilità la possibilità di riconoscere i più nuovi bachi scoperti.

Nessus è un sistema remoto, **composto da una parte server ed una client**. La prima è un demone disponibile solo per i più svariati ambienti Unix-like, come GNU/Linux, Bsd e Solaris. È il cuore dello scanner, in quanto si occupa di eseguire i test e simulare gli attacchi. Il client invece è solo un'interfaccia grafica per la configurazione e gestione di Nessus, ed è disponibile sia per ambiente Unix che per l'ambiente Windows.

Vediamo ora come si installa, configura e utilizza la versione Linux di Nessus per operare un controllo del proprio sistema.

La prima operazione da eseguire è ovviamente quella di ottenere i pacchetti contenenti il programma. **Si può scaricare dal sito ufficiale un pacchetto completo contenente lo script per la compilazione e l'installazione,** oppure una serie di archivi rispettivamente per il server, i plug-in, il client e le librerie necessarie, tutti quanti da compilare a mano. Noi seguiremo la prima strada, senza dubbio più veloce e pratica per chi si avvicina a Nessus la prima volta.





Una volta posto l'installer nella home dir, è sufficiente digitare (come utente) il comando:

```
$ sh nessus-installer.sh
```

Lo script si occuperà di configurare il sistema, compilare i programmi e installare il tutto nel modo migliore. Per alcune delle procedure è richiesta la password di utente root, senza la quale non è possibile portare a termine l'installazione.

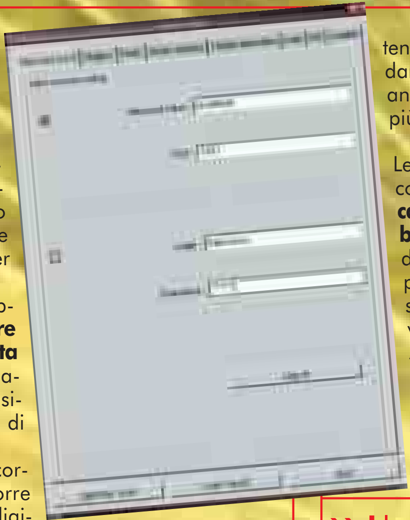
>> Il server

L'amministrazione del server **deve essere necessariamente effettuata dall'utente root**, in quanto gira con i privilegi mas-

NESSUS È UN OTTIMO TOOL GRATUITO PER TESTARE LA SICUREZZA DEI PROPRI SISTEMI DAL PUNTO DI VISTA DEGLI HACKER.

simi. La prima cosa che occorre fare è creare un certificato per le connessioni Ssl. A tal proposito viene fornito uno script completamente automatizzato: nessus-mkcert. Successivamente, attraverso il comando nessus-adduser è necessario inserire almeno un utente che possa collegarsi al server per eseguire gli attacchi.
Attraverso il comando nessus-updateplugin **è possibile inoltre mantenere aggiornata la lista dei plug-in disponibili**, così da cercare sempre tutti i buchi di sicurezza disponibili nella libreria di scansioni di Nessus.
A questo punto il server risulta correttamente configurato. Occorre solamente avviare il demone, digitando in questo caso, come utente root:

```
# nessusd -D
```

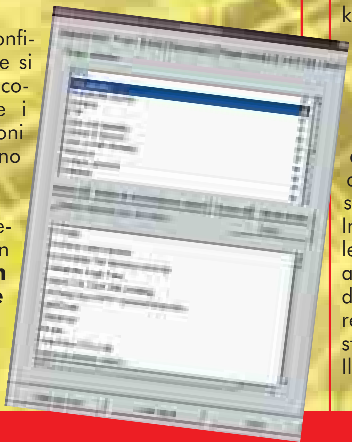


Plug-in: I plug-in sono dei moduli di Nessus che si occupano di eseguire gli attacchi veri e propri. Sono scritti in Nasl, acronimo di Nessus Attack Scripting Language, un linguaggio di programmazione specificatamente creato per scrivere test di sicurezza da utilizzare con Nessus.

>> Il client

Una volta configurato e avviato il server, **è possibile collegarsi da qualsiasi host esterno, se le regole del firewall lo permettono.**
La prima schermata che compare è quella che si occupa di richiedere di inserire i dati per la connessione e il login al server.

Una volta connessi, occorre configurare il tipo di scansione che si vuole effettuare. Come prima cosa, è necessario selezionare i plug-in contenenti le definizioni degli attacchi che si desiderano eseguire.



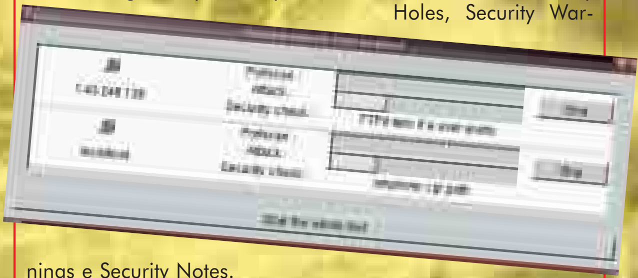
La lista è molto lunga e completa, e si arricchisce di versione in versione. **Alcuni dei plug-in possono potenzialmente mandare in crash il sistema testato**, così Nessus preferisce non abilitarli di default, mantenendo attivi solo quelli che non possono operare alcun danno. È comunque possibile in ogni momento attivare anche i moduli pericolosi, per eseguire una scansione più approfondita.

Le opzioni da configurare sono moltissime, ma per incominciare ci si può affidare a quelle di default. **L'unica opzione veramente importante è la selezione del bersaglio**, nella schermata Target selection. Se si desidera testare il proprio computer, occorre inserire semplicemente localhost, altrimenti è possibile digitare una serie di indirizzi IP o nomi di dominio separati da una virgola.
A questo punto tutto è pronto: basta fare clic sul tasto Start the scan per incominciare il test di sicurezza.

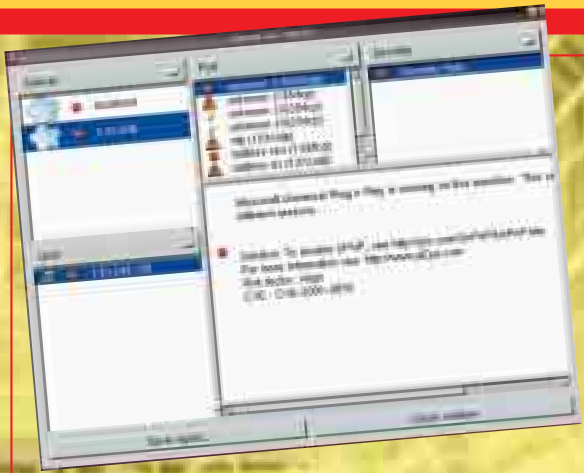
Il test può durare più o meno tempo, dipendentemente dalla banda disponibile, dal numero di host da verificare e da quanti plug-in sono attivi.

>> L'analisi dei risultati

Al termine di questa operazione, Nessus fornisce i risultati dei suoi test, suddivisi fra ogni sottorete e host. Il programma segnala quattro tipi di indicazioni: Serious, Security Holes, Security Warnings e Security Notes.



I buchi di sicurezza sono senza dubbio le falle cui occorre mettere una pezza per prime, soprattutto quelle classificate come serious. Sono spesso server con account di default o protocolli rinomatamente insicuri, tutte porte aperte anche ai cracker meno esperti. Nella descrizione del problema, **Nessus fornisce anche possibili soluzioni o indirizzi Internet ove è possibile scaricare le opportune patch**.
In ordine di importanza, seguono poi i warnings. Questi sono possibili problemi di sicurezza, anche se dal rischio molto basso. Sta poi all'esperienza di ogni buon amministratore di sistema decidere se seguire o meno queste indicazioni, in quanto spesso vengono indicati anche servizi che si desidera siano visibili dall'esterno.
Infine seguono alcune note di sicurezza, relative soprattutto alle informazioni sul sistema che un eventuale attaccante può acquisire. Sono le versioni dei server, le porte aperte, il nome dell'host e altri dettagli simili. Questi non compromettono direttamente il sistema, ma forniscono ad attaccanti esperti gli strumenti per studiare un attacco ben mirato.
Il report può essere salvato in vari formati per permetterne una

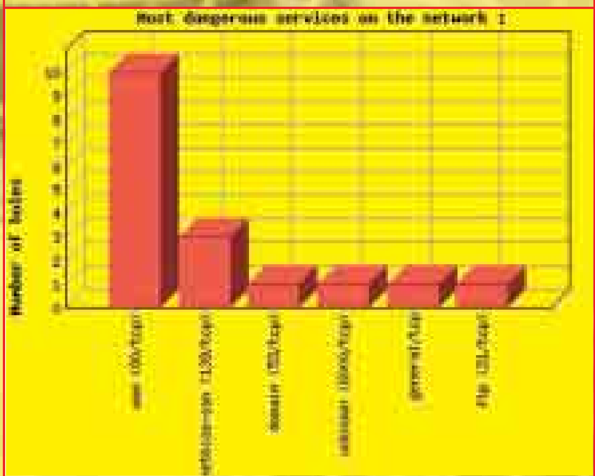


più approfondita consultazione. Fra le opzioni di salvataggio compare anche la possibilità di **creare un report dettagliato in versione Html**, con una serie di grafici che aiutano ad individuare i problemi e gli host più vulnerabili.

>> Fatene buon uso!

Nessus è un sistema potente e versatile, ma occorre prenderci un po' di confidenza per utilizzarlo al meglio. Da una parte **permette di riconoscere tutte le falle di sicurezza presenti sui propri sistemi**, suggerendone le possibili correzioni. Dall'altra parte permette di trovare falle e porte aperte in sistemi remoti, anche se difficilmente passerà inosservato uno scanning così intrusivo come quello effettuato da Nessus. In entrambi i casi i suoi risultati vanno correttamente interpretati, e **solo l'esperienza di ogni singolo utente può fornire la chiave di lettura corretta.**

Francesco "fra2k++" Facconi



Tutti i plug in di Nessus

Al momento attuale, per Nessus esistono circa 1900 plug in, ognuno specializzato per simulare un certo specifico attacco. Molti sono compresi nella distribuzione, ma altri più recenti pososno essere scaricati dal sito del programma (http://cgi.nessus.org/plugins). È possibile visualizzare la lista completa, quella che comprende solo i plug in aggiunti dopo il rilascio dell'ultima versione, o una lista strutturata per tipo di attacco. Le principali famiglie di plug in sono:

* Backdoor
* Abusi dei CGI
* CISCO
* Attacchi Denial of Service
* Abusi di Finger
* Firewall
* FTP
* Ottenere una shell da remoto
* Ottenere un accesso root da remoto
* Netware
* NIS
* Port scanner
* Accesso remoto ai file
* RPC
* Impostazioni
* Problemi SMTP
* SNMP
* Servizi inutili
* Windows
* Windows: gestione utente

È sempre consigliabile avere tutti i più recenti plug in installati quando si esegue un test, in modo da permettere a Nessus di riconoscere anche ultime falle di sicurezza scoperte. Il modo più semplice per avere la lista aggiornata è quello di digitare in shell sul sistema dove è installato il demone, come utente root, il comando nessus-update-plugins, che si occupa di cercare tutti gli aggiornamenti, scaricarli e installarli correttamente nel sistema. In alternativa, è possibile scaricare dal sito di Nessus ogni singolo plug in, che non è altro che uno script in linguaggio NASL. Una volta avuto il file, occorre copiarlo nella directory dove risiedono i plug in, che in generale risulta essere /usr/local/lib/nessus/plugins/. Infine ricordiamo che è meglio riavviare il demone nessusd.